What will be the future of data flows between the EU and the UK post-Brexit?

Laurence Sean Lawson
Faculty of Law, University of Helsinki
MICL Thesis
Student number: 014609895
18.10.2018

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto - Fakultet/Sektion – Faculty		Laitos - Institution – Department
Faculty of Law		
Tekijä - Författare – Author		
Laurence Sean Lawson		
Työn nimi - Arbetets titel – Title		
What will be the future of data flows between the EU and the UK post-Brexit?		
Oppiaine - Läroämne – Subject		
Data Protection Law		
Työn laji - Arbetets art – Level	Aika - Datum – Month and year	Sivumäärä - Sidoantal – Number of pages
Master's	October 2018	78

Tiivistelmä - Referat – Abstract

Never has there been a more interesting time to be invested in the actions of the European Union, it seems that the organisation is involved in nearly every event occurring on a global stage. Wherever an individual or business is based, the European Union is likely to have had some sway on their way of life. This paper seeks to tackle two of the hottest legal topics within the European Union, namely the General Data Protection Regulation, an overhaul of privacy law never seen before and Brexit, the United Kingdom's impending departure from the European Union. As the relationship between the United Kingdom and the European Union is due to undergo a seismic shift, this paper will evaluate what will happen in terms of the flow of personal data between the two under several different scenarios.

For the first part of this paper, I will assess the current situation, and how all parties find themselves in such a predicament. It will then consider the impact that Brexit and the General Data Protection Regulation have had upon each other as of this date, and what is to be expected of both before the United Kingdom's formal departure from the European Union. This will provide a key oversight into the topic in question and assist in laying the groundwork for parts 2 and 3.

In the second part, I will discuss the possible outcomes from what has been coined as a 'soft Brexit'. For this, I will evaluate the current possibilities that bear some credence and use this, in tandem with agreements the European Union has struck with other nations for data transfers to provide insight into the likelihood of such an occurrence along with how such an aim can and could be achieved.

For the third part, I will discuss the possible outcomes arising from what would be classed as a 'hard Brexit'. In this section, I will continue the theme of looking at mirroring a deal the European Union has previously struck with one of its allies, the United States, along with the backups should such a system fail or not be deemed suitable. By looking into the potential transfer mechanisms where no other deal is in place, I will be able to assess the benefits and pitfalls of a British-based business implementing such a system when there is no agreement in place between governments.

Finally, in the conclusion, I will review the discussed options, taking into account their likelihood, difficulty of implementation, and using statements from those in positions of power to provide insight into what is the most likely option, which options should be a preference, avoided, and considered. Following this, I will also provide my own, personal recommendation that has been garnered from the research and review of this paper to add further insight.

Avainsanat – Nyckelord – Keywords
Data Protection Law, Privacy, GDPR, Data Transfers, International Data Flows, Transfer Mechanisms, Privacy Shield, Safe Harbour, Model Clauses

Säilytyspaikka – Förvaringställe – Where deposited

University of Helsinki E-Thesis Database

TABLE OF CONTENTS

1 INTRODUCTION

The year 2016 saw a plethora of turbulence across both the political and legal landscapes, with a range of key events seeking to change the very nature of how daily life is conducted. Perhaps one of the most oft discussed and debated of these was the United Kingdom's somewhat surprise decision to leave the European Union (EU) in June 2016 via a referendum. With the UK's expected departure from the EU set to formally occur in March 2019, there will be a seismic shift in the manner of operations within not only the UK, but also the EU and the world as a whole.

On the other side of the English Channel, in Brussels, the EU also undertook its own large-scale change to how it operates at its core, officially passing the General Data Protection Regulation[1] (GDPR) to bring around what some have hailed as "the largest change in digital law ever seen"[2]. Scholars, experts, law students, and the general population have all acknowledged that the GDPR itself will affect not only Member States of the EU, but also any company which seeks to process the data of EU citizens, "regardless of whether the processing takes place in the Union or not"[3].

Some critics of the GDPR have taken issue with this, believing that the EU has overstepped its bounds and is, in effect, acting as a "world data police"[4], whilst others have hailed it as the "gold standard" for data protection law[5].

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[2] https://www.theguardian.com/legal-horizons/2017/dec/14/gdpr-the-new-data-protection-law-giving-watchdogs-a-mega-bite accessed 07.05.2018
[3] GDPR, Article 3
[4] J. Stanganelli, GDPR Territorial Scope: Location, Location, Location?, 2018
[5] G Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016) 6 International Data Privacy Law, 77–78

While these facts are somewhat hard to disprove as the EU have stated that they want to "reshape the way organizations across the region approach data privacy"[6], the eventual impacts that this revolutionary piece of law will bring haven't even begun to scratch the surface.

It is also the opinion of the EU that "companies recognise that strong privacy protections give them a competitive advantage… [leading to the fact that] many, especially those with [a] global reach, are aligning their privacy policies with the GDPR, both because they want to do business in the EU, and because they see it as a model to follow."[7] When this is coupled with the EU stating that, as an organisation, they "should seize this opportunity to promote its data protection values and facilitate data flows by encouraging convergence of legal systems"[8], a picture of their ambitions starts to form.

While it remains an EU Member, the United Kingdom is expected to abide by the rules of the GDPR in their entirety until their departure is formalised. With a long list of recitals and articles, the GDPR is highly complicated and has a broad range of features.

The true question comes from the fate of the UK Data Protection sector once the UK formally leaves the EU. With negotiations ongoing, and a wide array of options on the table, a cornucopia of possibilities are available for the UK and EU present themselves. Each one of these options could lead down a rabbit hole of legislation, mechanisms, and changes will strike the very heart of the British business sector that wishes to continue to operate within the borders of the remaining 27 Member States.

Both the GDPR and the United Kingdom's departure from the EU are highly complex subjects, with a rich history and a foggy future, especially when it comes to how the two will interact with each other. To gain a further understanding as to where these two could lead, and meet, it is important to discuss what each are and how they reached their current status.

[6] https://www.eugdpr.org accessed 07.05.2018
[7] Communication from The Commission to the European Parliament and The Council: Exchanging and Protecting Personal Data in a Globalised World
[8] Ibid

2 BACKGROUND

2.1 Overview of GDPR

At its core, the GDPR is an overhaul of Data Protection law within the 28 Member States European Union. Prior to the GDPR, the European Union relied heavily upon a Directive from 1995[9], which brought its own inherent flaws. Included in this was the lack of harmony between member states[10] due to the very nature of Directives being the imbalance between nations, and the lack of rights that it brought[11]. Indeed, this lack of rights led to the EU applying some common law rulings in order to somewhat try to keep up with the advancement in technology and changing attitudes towards privacy[12].

The main purpose the GDPR seeks to establish key rights for individuals regarding their data[13] and bring in penalties for non-compliant organisations[14] of up to 20,000,000€ of 4% of turnover[15] meaning that these penalties can, in theory, be unlimited.

Obviously, there is a lot more to the GDPR than rights and money, but with the GDPR consisting of 99 articles and 173 recitals, the sheer scope of the legislation can lead to many scholars losing track of the important issue of protecting the data of individuals.

For the purposes of this paper, the dissection will take place in the areas regarding data transfers and data flows, the various options available, and an attempt to read between the lines to determine the full intent and possibilities available for these transfers.

---

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[10]Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"
[11] The GDPR is bringing in several new rights, including that of Data Portability, which did not exist in the 1995 law
[12] For example, see Google v Spain (Case C-131/12)
[13] GDPR Chapter 3
[14] GDPR, Article 83
[15] Ibid

2.2 Overview of Brexit

On the other side of the coin lies the second influencing factor for this paper, namely Brexit. As mentioned, the United Kingdom's citizens opted to leave the EU through a referendum. Many individuals were shocked by this decision, and experts and markets found themselves in a state of confusion following this result.

2.2.1 How did we get here?

To determine how the United Kingdom found itself in the position wherein the populous elected leave the European Union, it is worthwhile to view the EU, its history, and how it evolved.

It can be said that the EU's origins are found in 1950 with the Schuman Declaration[16], which sought to create a common market for European Coal and Steel, under the idea that if nations were economically tied, then this would "make war not only unthinkable, but materially impossible"[17]. This Declaration was fulfilled when, in 1952, the European Coal and Steel Community was established.

The success of this agreement saw the Member States move to integrate further, instigating the Treaty of Rome[18] in 1957, which created the European Economic Community (EEC), the true precursor to the EU. The initial members of the EEC were Belgium, France, Italy, Luxembourg, and West Germany. While initially designed as a customs union, the EEC expanded rapidly to include other aspects such as a common agricultural policy.

The success of the EEC saw several other nations apply for membership, including the United Kingdom, who found their membership application vetoed by French president Charles de Gaulle in 1963, with the now infamous statement *"l'Angleterre, ce n'est plus grand chose"* (England is not much anymore), and once more in 1967. These rebuffs only seemed to motivate

[16] Declaration of 9 May 1950: The Schuman Plan for European Integration
[17] Ibid
[18] European Union, Treaty Establishing the European Community, Rome Treaty, 25 March 1957

the British who eventually found themselves joining the EEC with the Republic of Ireland and Denmark in 1973, following the retirement of de Gaulle.

From the beginning of its EEC membership, the UK was always granted something of a 'special status' within the Community. Of course, both the economic and political power the UK possessed led to "concerns and tensions within other the Member States"[19]; a precursor to what would come.

Despite this, the UK still held a referendum on its membership as early as 1975, a mere 2 years after joining. Unlike the most recent one in 2016, this need for a referendum was caused more from political infighting from within the traditionally working-class Labour party (who officially sided with remain for the 2016 referendum) rather than the Conservative party who are currently responsible for handling the UK's departure. The result of said referendum was a resounding vote to remain a Member, with 67.2% voting that way[20]. Despite this overwhelming victory, it did set in motion the basis for a turbulent relationship between the European landmass and the United Kingdom.

As the EEC continued to grow in membership and scope to encompass European health, environment and, critically, legal affairs, it sought to solidify these changes in the Maastricht Treaty[21], signed in 1992 and enforced in 1993, and the EEC became known as the European Union. Indeed, this 'special status' for both the UK (and Denmark) was evident within the Maastricht Treaty[22]. Following this, the EU saw rapid expansion, both in scope and members, reaching 28 Member States[23], and closer trade ties, exemplified by 19 of the 28 Member States entering into a single currency, the Euro, and its adoption being a requirement of all new applicants.

[19] Salmaso, Alfredo. (2016). A Soft Brexit: Analysis of the referendum outcomes and future possible scenarios. 10.13140/RG.2.2.27697.58723.
[20] House of Commons Library: Briefing Paper 7253 (13 July 2015): The 1974-75 UK Renegotiation of EEC Membership and Referendum
[21] Treaty on European Union, Treaty of Maastricht , 7 February 1992
[22]Denmark obtained opt-out from the Maastricht treaty, outlined in the Edinburgh treaty: including not joining the single currency, control over monetary policy, and not bound by the UEM rules, as did the UK
[23] As of July 2018

This concept of increased powers within the EU over Member States led to a great deal of concern within some current Members, most notably the UK, which has always maintained an air of independence. This independence is evidenced through keeping its own currency, opting out of the Schengen agreement, and considerable efforts to hamper the passing of EU legislation that it felt did not suit national interests.

This, of course, coincided with a political wave within the United Kingdom that gained traction, namely the rise of a new political party within the UK, the United Kingdom Independence Party (UKIP). The sole purpose of this party was the detaching of the UK from the EU. Once considered a small party, UKIP saw itself cast into the political stratosphere in 2014 during the European Parliament elections where they topped the poll amongst voters to represent British values in Brussels[24], breaking the duopoly of the Conservative and Labour parties.

This rise continued on the domestic front too, with the party obtaining close to 4 million votes (12.6% of the total vote) in the 2015 general election[25]. This saw the party unseat the Liberal Democrats as the 3rd largest party by votes within the UK, a result which drew alarm from some sections, as the Liberal Democrats had been used to form a government in the 2010 election with the Conservatives.

Under pressure from this burgeoning section of the electorate, and from his own party, the Prime Minister at the time, David Cameron, made a pledge in his manifesto to hold an in-out referendum on EU membership should he be re-elected and be able to form a government without the need of another political party[26].

Due to several factors, potentially including the referendum pledge, the Conservative party, and David Cameron, retained power. As expected, this culminated in the UK holding a non-binding

[24] http://www.europarl.europa.eu/elections2014-results/en/country-results-uk-2014.html
[25] Electoral Commission, 2015 UK General Election Results: https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/uk-general-elections/2015-uk-general-election-results
[26] Conservative Party Manifesto 2015, pg 30: http://ucrel.lancs.ac.uk/wmatrix/ukmanifestos2015/localpdf/Conservatives.pdf

referendum as to whether the country should remain a member of the EU or leave. The term adopted by the media, and subsequently by all audiences was 'Brexit', a portmanteau of 'Britain' and 'Exit'.

Said referendum was held on the 23rd of June 2016, with over 30 million individuals casting their vote and with a turnout rate of 72.2%[27]. After all the votes were counted, the official result determined that 51.9% of the votes were to leave the EU, compared to 48.1% who chose to remain[28]. This result also meant the end of David Cameron's tenure as Prime Minister, as he resigned the following day after he unsuccessfully campaigned to remain.

Whilst non-binding, the British government at the time took this as a clear mandate from the British populous as to what was needed to do; namely leave the EU. The process of such a withdrawal is briefly described under a later piece of European legislation, Article 50 of the Treaty of Lisbon[29], which states that "A Member State which decides to withdraw shall notify the European Council of its intention"[30], upon which the Member State (UK) has "two years after the notification"[31] before exiting to enable the relevant negotiations for withdrawal. Under mounting pressure from those who voted to leave, especially within her own government, the British Prime Minister invoked Article 50 on the 29th of March 2017; leading to the UK's planned departure date being at the end of March 2019.

As mentioned, under the terms of Article 50, a Member State will cease to be a Member 2 years after submission, regardless of the state of negotiations. If, as some have suggested is a possibility, there is no full deal between the UK and the EU by such a date, this will lead to an immediate cessation of EU policies, support, and, crucially, legislation; a term dubbed the 'cliff-

[27] Obtained from Electoral Commission: https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information
[28] Ibid
[29] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007
[30] Ibid, Article 50
[31] Ibid

edge' or a hard Brexit. The potential of a hard Brexit remains a possibility and, as mentioned by the British Prime Minister "no deal is better than a bad deal"[32].

Of course, for some, a no deal situation is the worst possible outcome, but, with time still on the clock in terms of the UK's membership, discussions can take place as to how every aspect of EU membership will be affected by Brexit. Key to these for businesses purposes is the previously mentioned GDPR.

2.3 Impact of Brexit on the GDPR

Of course, with the UK government and the EU agreeing a departure date for late March 2019, the UK will have been under the direct influence of the GDPR for nearly a year. It will also continue being an active member of the European Union's newly formed European Data Protection Board (EDPB)[33] through the Information Commissioner's Office (ICO), a role that it was lauded for under the previous guise of the Article 29 Working Party. During this membership window, ICO will discuss matters relating to the correct application of the GDPR and resolving conflicts between supervisory authorities along with providing more detailed guidance on some of the more contentious aspects of the GDPR.

As the GDPR came into force while the United Kingdom is a member of the European Union, there was the potential for the British government to enact a variation of the GDPR into national law to allow for GDPR deviations, including changing what the age of a child is and freedom regarding the potential for criminal sanctions.

For the United Kingdom, they triggered this potential through the Data Protection Act[34], an act that received Royal Assent and became law days before the GDPR was fully enacted on the 25th of May 2018. This Act will continue to be enforced once the UK leaves the EU and will govern how data is protected post Brexit; part of the reasoning for this was to ensure that the nation's

[32] Interview with Theresa May by Jeremy Paxman: 29.05.2017: https://news.sky.com/video/may-on-brexit-no-deal-better-than-a-bad-deal-10897952
[33] GDPR Article 68
[34] Data Protection Act 2018

data protection framework is “suitable for our new digital age, allowing citizens to better control their data.”[35]

However, under the provisions of Article 50[36], the UK will cease to be an EU Member State at the end of March 2019 and, as such, will no longer be subject to the direct applicability of EU laws, including the GDPR. As such, the UK Data Protection Act will work as the sole source for UK Data Protection Law. This act can be seen as the UK attempting to have something on the table to present to the EU post Brexit to demonstrate that they have the objectives of the GDPR close to their hearts.

At this point, unless an agreement is reached, the UK will be classified as a ‘third country’ under the terms of the GDPR and therefore will be part and parcel to the stringent restrictions regarding the transfer of personal data beyond the borders of the EU[37]; and therefore entirely beholden to the mechanisms reserved for nations with more turbulent relationships. If the cliff edge does happen, this would lead to the awkward situation of legal data transfers to the UK being prohibited the next day[38], unless alternative measures are brought into play. The effect of such a change will be monumental, affecting businesses small and large alike, along with the allure for businesses when deciding if they should base operations within the UK.

In tandem with this, due to the scope of the GDPR under Article 3, many businesses in the UK will still be bound by the rules of the GDPR should they wish to continue operations with their EU counterparts; tethering them to the system which many had issues with.

Furthermore, the status of ICO within the EDPB will also be rescinded, leading to a lack of influence within the framework they helped create. Indeed, the EU has acknowledged that “The

[35] Statement by HRH. Queen Elizabeth II at the UK Parliament in June 2017
[36] Article 50 of the Lisbon Treaty
[37] GDPR Articles 44-50
[38] GDPR Article 44

UK has been a key player in shaping policies in this area"[39], despite offering stark opposition to some directives on occasion[40].

[39] "The Implications of the United Kingdom's withdrawal from the European Union for the Area of Freedom, Security and Justice, Committee on Civil Liberties, Justice and Home Affairs", December 2017:
http://www.europarl.europa.eu/RegData/etudes/STUD/2017/596824/IPOL_STU(2017)596824_EN.pdf

[40] An example of this is the now invalid Data Retention Directive: DIRECTIVE 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

3 EVIDENCE AND RESEARCH

The importance of such a study into the effect of the GDPR and privacy law in general outside of the borders of the European Union is not to be understated; and, with the UK seemingly heading into this area, the influence of the EU over the UK post-Brexit could still be substantial.

Even the European Union has alluded to this rapid shift and need to overhaul the status quo of data privacy law. Indeed, they have stated that "several countries and regional organisations outside the EU, from our immediate neighbourhood to Asia, Latin America and Africa, are adopting new or updating existing data protection legislation"[41] to deal with "the growing demand for stronger data security and privacy protection"[42]. While it may not have been relevant at the time, a great deal can be drawn from the first part of that statement, with the UK about to fall into the "immediate neighbourhood"[43].

In the same statement, the EU have acknowledged that they should "proactively engage with third countries in this matter"[44]; of which the UK is likely to find itself unless a deal can be arranged.

As alluded to earlier, the European Union is seeking to place itself in the position to be the central pillar of this change, letting other nations work around the European model. Therefore, it will be of the utmost interest to see if the European Union is full of bluster in this regard, or if their statement has credence and they will be highly restrictive as to with whom they allow the free flow of personal data.

While, under the Great Repeal Bill[45], the government of the UK will maintain several EU laws, many EU laws applicable to the UK will face the proverbial chopping block. These changes

[41] Communication from The Commission to the European Parliament and The Council, Exchanging and Protecting Personal Data in a Globalised World COM/2017/07 final
[42] Ibid
[43] Ibid
[44] Communication from The Commission to the European Parliament and The Council, Exchanging and Protecting Personal Data in a Globalised World COM/2017/07 final
[45] HC Bill 5 2017-19

could see the UK's reputation in the eyes of the EU cast into some doubt; and with it the potential for further disruption to data flows between the two. This reputation is highly important to the UK, which boasts a highly developed economy predicated upon the financial services and technology sectors, both of which are likely experience the most severe adverse effects of a disrupted data flow. Indeed, such a potential hindrance to day-to-day operations has seen leading British organisations like HSBC look into moving large swathes of the business abroad in order to continue to reap the benefits of EU membership[46]

[46] https://uk.reuters.com/article/uk-britain-eu-hsbc/hsbc-shifts-european-branches-to-french-unit-control-ahead-of-brexit-idUKKBN1KT1G1 accessed 26.09.2018

4 METHODOLOGY

The field of legal research is a complex discipline and there is no clear accepted method to conduct such an investigation, especially one wherein a clear theory is not presented. Much of the dissection therefore comes down to the author's own personal beliefs and whichever approach will be most apt for the scenario mentioned. While the majority of this paper will seek to avoid the encroachment of my personal thoughts on both the GDPR and Brexit, it is important that my own views in regards to legal research emerge.

For this paper, I will mainly utilise a legal dogmatics approach, otherwise known as Rechtsdogmatik. This will involve conducting a review of the law itself and the surrounding material to predict an outcome that would be in line with what the deciding powers will opt for in a post-Brexit scenario. This theory is based in the idea that "the law is a continuation of politics by other means"[47] which would appear to be the most apt methodology for discussing the GDPR's relationship with Brexit, both of which are highly political in origin, as discussed during the introduction.

Indeed, this theory implements a method that systematically and analytically evaluates the law as it is transcribed. As the secondary name suggests, this approach is far more befitting a continental European approach instead of the approaches found within the Anglo-American legal systems. This is one of the reasons as to why this approach was selected. While it is clear that the Anglo-American legal theories, which I have studied, will play their role in terms of an application of case law to make points, a Continental European approach is the preferred course for the overarching agenda.

Legal dogmatics has been described as consisting of five core elements: Firstly, a collection of legal assumptions (for example, that the GDPR applies to all EU Member States); secondly that there are assumptions regarding the object of the laws (for this paper, that would be the field of data protection); the third element is stating which laws are admissible (for example, the GDPR

[47] Álvaro Núñez Vaquero, Five Models of Legal Science, *Revus*, 19, 2013, pg. 53-81

is, whereas defunct legislation is not), fourthly that there are methodological rules regarding the steps taken to move from sources to interpretation; and finally, a number of value assumptions.[48]

In terms of gathering sources for review and critique, this paper will primarily rely upon EU law (such as the GDPR) and national legislation where available (such as the UK Data Protection Act). However, the realistic view is that these may not wholly suffice due to the shifting nature of both law and the current negotiations, and, as such, this paper will secondarily consider guidance materials from established bodies. These established bodies include, but are not limited to, the Article 29 Working Party (and its successor), the Information Commissioner's Office et al., or established methods of statutory interpretation such as Hansard and Committee meetings for British laws. As part of third-tier sources, where neither primary nor secondary sources provide an insight, this paper will consider academic commentaries and statements made by individuals or organisations; with significant weighting given to said individual or organisation's expertise or standing within the field.

In addition to this, this paper will also draw upon the legal interpretation mechanisms established within the British legal system (The Literal, Golden, and Mischief rules). This is largely due to the longevity of said mechanisms within the legal research field, and the influence that the British have had upon the European Union's legal system. Indeed, two of the British mechanisms (the Golden and Mischief rules) can be seen as working in the same way as the commonly used EU approach, the teleological approach. This approach has the ultimate aim of seeing the intent of the legislator when enacting the rule and not specifically the text itself. Truly, the teleological approach is the most common method of the European Court of Justice concerning interpretation of legal provisions[49], therefore such an approach within this paper makes sense as this utilisation will mean both EU and UK legislation can be viewed through essentially equivalent lenses. However, as much of this paper will focus on the EU perspective, due to the GDPR being the overarching law to be studied, other EU mechanisms will be utilised to draw out conclusions; which are still permissible under the British mechanisms[50]. While this may seem like an odd

[48] Aulis Aarnio, Reason and Authority, pg. 82–83
[49] Van Hoecke, M., Law as Communication, 2002, p. 144
[50] For example: Pepper v Hart [1993] AC 593

combination to utilise in order to provide the best possible prediction for a post-Brexit world, the intersection between both European and British standards is precisely what should allow the clearest image to present itself.

Due to the nature of interpreting the law, this paper will use all the relevant tools available to ensure a lack of bias, which may be common within such a heated topic. This will be accomplished through using logical deductions, interpretation of the language within the sources, and personal knowledge on the topic garnered from experience to draw out the most accurate view of each aspect discussed. By utilising these tools, the result should be a firm foundation to provide what can be considered as educated a guess as is feasible for each of the scenarios to be mentioned below.

4.1 Structure of the Paper

To fully ascertain what impact Brexit will have on data flows between the UK and the EU in a post-Brexit world, the current available options must be assessed on their likelihood. At the time of writing, negotiations are still ongoing between the parties and nothing is set in stone in terms of what can be expected. Therefore, the best recourse to perform this act is to objectively look at the GDPR's allowances for transfers to non-EU nations through agreements, treaties, and articles, how this structure is built, and if the UK could successfully adopt any of these options.

Firstly, this paper will look at the scenarios that could arise if the UK is considered successful in negotiations with the EU and has some form of deal before the deadline, the Soft Brexit. This would mean the UK and the EU have parted on relatively good terms and relations are cordial. By looking at how other nations with cordial relationships interact with the EU, the hope is that the UK can draw from these examples to implement their own system. These systems will be analysed and compared to the UK's situation to better cast a light on what could be done. In order to not have an inordinate length, only a few nations will be chosen as examples, based on their relevance to the UK's predicament.

The second scenario, which is the default option, is a Hard Brexit. This would mean that the UK and the EU failed to reach any form of agreement before the deadline and the UK finds itself in the same grouping as nations without a close connection to the EU. To analyse the impact this would have, this paper will view how the GDPR allows data transfers to nations in this category and, by applying these mechanisms to a UK-based business, clear assistance can be obtained and prepared for.

As Brexit, by nature, is a complicated topic, there is no singular answer that would solve all issues; but several options have been publicly touted by senior individuals who have their roles to play within the negotiation process.

By looking at each available method, combined with the scenario that would lead to the potential for it to be adopted, one can provide an educated guess as to which options are the most plausible and which act as mere pipe dream.

5 OPTIONS ON THE TABLE

As mentioned earlier, Brexit is not simply a trivial concept or process, it is a complex and largely misunderstood topic. The EU is highly integrated into the core of the UK's activities. There is no one route to the UK's departure, just as there is no one route to how the UK will adapt to ensuring the free flow of data with the EU after such an event.

To better understand what the future of the UK-EU data flow relationship post-Brexit, all these possibilities must be checked, reviewed, assessed, and evaluated not just to their possibility, but also for any other repercussions.

5.1 Soft Brexit

The first method of Brexit is the so-called 'soft Brexit'. This method has varying degrees as to what it could constitute. However, all iterations of a soft Brexit feature a multi-stage process of departure, including the opportunity for deals along the way that could see some resemblance of the UK keeping ties with the EU; be that a trade agreement, membership to other blocs, or deferring the end date to pass other legislation to minimise the impact of Brexit in general. Utilising this method would allow time for both the UK and the EU to determine what kind of long-term relationship would best serve the interests of both sides.

A drawback of this is that, with a deferral, it would require the remaining 27 EU Member States to agree to every term; something that may be difficult due to the complexity of the deal, and, especially when considering how long it took the Member States to agree upon the trade deal with Canada.

5.1.1 EEA Membership

One option on the table for the UK to mitigate the issues regarding data protection post Brexit would be to exchange their EU Membership for membership into the European Economic Area (EEA); potentially the softest of all Brexits. The EEA is a system consisting of all current EU Member States along with three of the four European Free Trade Association (EFTA) members (Iceland, Liechtenstein, and Norway), all of whom have strong historic ties with the EU; Switzerland is the only member of the EFTA which is not part of the EEA.

The EFTA is "an intergovernmental organisation set up for the promotion of free trade and economic integration to the benefit of its four Member States – Iceland, Liechtenstein, Norway and Switzerland – and the benefit of their trading partners around the globe"[51], founded in 1960 in Stockholm[52]. This, of course, means that the aforementioned nations are not members of the EU, despite their close geographical and political relations with a variety of EU Member States and stark similarities between the political and ideological goals.

To maintain this independence while retaining a strong bond with EU Member States was, a workaround method opted into by the governments of Norway, Iceland, and Liechtenstein, was to join with the EU through the EEA Agreement[53] in 1994. The crux of this agreement was to guarantee equal rights and obligations for both businesses and individuals across all EU members and the three aforementioned nations, while not committing to full membership of the EU. Essentially gaining some key advantages such as free movement and some adherence to the pillars upon which the EU is built while avoiding some pitfalls such as a commitment to adopting the Euro as their currency.

[51] 'The European Free Trade Association' (EFTA no date): http://www.efta.int/about-efta/european-free-trade-association
[52] Ibid
[53] 'Agreement on the European Economic Area' (EFTA 1 August 2016): http://www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf

In terms of the application to data protection law, the three EFTA nations mentioned were included within the scope of the previous law[54]. Meaning that, like all EU Member States, the EFTA nations were required to implement their own national laws that enacted the aims of the Data Protection Directive into national law.

By being an organisation closely linked with, but not part of, the EU, the EFTA is subject to adverse decisions by the EU, without having a voice at the table. These decisions also include the topic of data transfer mechanisms and protection beyond EU borders. This severe drawback could be an obstacle for the UK as this could see the influence of their own authorities reduced on the European stage.

Of course, not all EU legislation automatically applies to the EEA; it requires a lot of oversight and a meeting of the EEA Joint Committee[55], featuring both EU and the three aforementioned EFTA members where they discuss the potential applicability of planned EU legislation to their territories. Although it can be seen that the vast majority of EU laws are transposed and passed by the EEA Joint Committee[56]; while the reasons for this lack of resistance is not given, it could be seen that these nations either work with the same ideals of the EU, or wish to have as few restrictions between them and their neighbours as possible.

For GDPR purposes, Article 44 is the key section when viewing the EEA relationship, stating that data should not be transferred to third countries who lack adequate protection. In a similar vein to the previous EU law on the topic[57], there is no mention towards the three EFTA EEA members.

This, of course, would mean that the EEA Joint Committee would need to formally approve the extension of the GDPR into their framework; and to air any grievances that may arise. In July of

[54] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[55] EEA Joint Committee (EFTA no date) http://www.efta.int/eea/eea-institutions/eea-joint-committee
[56] According to a review of previous meeting documents, all of which can be found at: http://www.efta.int/eea/eea-institutions/eea-joint-committee/eea-joint-committee-annual-reports
[57] Ibid 40

2018, six weeks after the GDPR came into full effect, the EEA Joint committee made its decision, formally adopting the GDPR into its own codes of conduct[58]. The result of this is that the members of the EFTA now follow the GDPR as if it were their own law.

EEA membership could therefore be considered an option for the UK in a post-Brexit world if the aim was to remain somewhat independent of the EU while also ensuring the free-flow of personal data to the EU and EEA members in general. This task will not be too cumbersome for the UK, as they would also need to accept the aforementioned decision, and continue to follow the GDPR as they would have done between May 2018 and the pencilled in Brexit date in March 2019.

It would also mean that it gains key trading partners in terms of the EFTA Member States, something that would be invaluable at a time when new trade deals would need to be negotiated following the cessation of the UK's EU membership. In tandem with this, the three EFTA members all share common traits within their economies to the UK. Both Norway and the UK drive a large amount of revenue from the North Sea oil reserves, Liechtenstein has a finance-driven economy and Iceland utilises fishing and states that fishing quotas are an issue with them regarding their application for EU Membership. A free trade deal with these nations would be highly advantageous for the developed sectors of the British economy.

In addition to this, it would require the least amount of effort from the UK government in terms of overhauling laws and rules that are in place. By adopting EEA membership, there will be minimal disruption across several sectors, including trade, finance, and free movement of labour.

As expected, there are some drawbacks for the UK for a proposed membership into the EEA. The most key of these is one of the main catalysts for Brexit as a whole, namely the financial contributions expected by the EU. One of the key campaign slogans from the Leave campaign was to use the estimated £350 million sent to the EU each week for its own national health

[58] Decision Of The EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audio-visual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]

service instead. However, studies estimate that EEA members will be expected to pay 3.22 billion Euros to the EU between 2014 and 2020 for joint programmes[59]; a figure that will substantially increase should the UK apply for, and be successful with, EEA membership due to the size of their economy. Indeed, even taken on an individual level, Norwegian citizens paid on average £106 per capita for their EU contribution in 2011, marginally lower than the UK's current figure of £128[60], meaning that UK contributions per person will remain at a somewhat similar level should EFTA membership be achieved. It is likely that this would cause furore within both the UK populous and Parliament.

One more drawback of the UK joining the EEA would be another of the motives for the decision to leave the EU, namely the concept of sovereignty; the control over their own laws and destiny. As previously mentioned, the EEA is beholden to many EU laws, especially regulations, to ensure a smooth relationship with the EU. In essence, having to obey the EU's rules without being able to voice their opinions at the time of conception. Of course, the Joint Committee can still weigh in, but a clear rejection within the Joint Committee is unlikely.

EEA membership would have one drawback that the UK would not like to see, namely the wish to see the ICO retain its status as a member of the EDPB. This is an attribute not granted to any of the incumbent EFTA members and a stance that the EU is not willing to change as it could open the potential floodgates for more outside agencies to interfere with EU policies. This feature would not be ideal for a large swathe of the British data protection community and those who rely on the ICO being an approved supervisory authority for GDPR purposes. As it stands, despite the close connection and the decision to implement the GDPR in their framework, no EFTA or EEA member is permitted to sit on the EDPB.

Indeed, the individual responsible for leading Brexit negotiations from the EU perspective, Michel Barnier, has gone on record to state that he was concerned about this admittance due to worries about "Who would launch an infringement against the United Kingdom in the case of

[59] EU Programmes with EEA EFTA Participation (EFTA no date): http://www.efta.int/eea/eu-programmes

[60] House of Commons (2013), 'Leaving the EU', Research Paper 13/42, 1 July 2013.

misapplication of the GDPR? Who would ensure that the UK would update its data legislation every time the EU updates the GDPR? How can we ensure the uniform interpretation of the rules on data protection on both sides of the Channel?"[61]

These clear drawbacks could be part of the rationale as to why the British government has repeatedly stated that it has no intention whatsoever of applying for EEA membership. This point was made most fundamentally clear in a report it published in 2017[62], where it mentions that "The Government will prioritise securing the freest and most frictionless trade possible… [but] we will not be seeking membership of the Single Market"[63].

While it would solve some of the key data flow issues, this statement is the final nail in the coffin for the EEA system. There are, however, other ways of working around the issue of EU-UK data transfers post-Brexit; and with a softer Brexit, just not as soft as EEA membership.

5.1.2 Swiss System

One potential system is to mimic that of the other EFTA member who is not a member of the EEA, Switzerland. Due to its location, Switzerland is considered a highly important partner of the European Union. The EU is Switzerland's main trading partner and Switzerland forms the third biggest trading partner for the EU[64].

[61] Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE), 26th May 2018: http://europa.eu/rapid/press-release_SPEECH-18-3962_en.htm
[62] HM Government, 'The United Kingdom's exit from and new partnership with the European Union' (gov.uk 2017): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/589189/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Print.pdf
[63] Ibid Chapter 8
[64] http://ec.europa.eu/trade/policy/countries-and-regions/countries/switzerland/

Despite not being a member of either the EU or EEA, Switzerland has adopted various provisions of EU law to be part of the European Single Market and has a free trade agreement with the EU[65] to allow the free movement of goods, people, services and the like across borders.

As expected, this free movement also extends into the digital and data worlds, with Switzerland the holder of an adequacy decision[66].

The topic of adequacy is not something just brought about by the GDPR either, the topic of finding adequacy and the mechanisms for such are long established concepts arising from the previous Data Protection Directive[67], which is what was granted to Switzerland.

In terms of this scheme, third countries reach out to the European Commission in an effort for the Commission to recognise their data protection system as being "essentially equivalent"[68] to that of the EU; once granted, it enables personal data to flow freely between the EU and the third country without the requirement of other safeguards.

Adequacy decisions can either granted to cover all aspects of personal data, or, if the Commission has concerns about aspects, be restricted to sectors. Switzerland, along with the majority of third nations holding adequacy, fall in the former.

Further to this, the Commission broke down these adequacy decisions further in 2017[69], based largely on the applicant's motivation for gaining adequacy. Switzerland found itself within the first of the three categories, namely nations that are "closely integrated with the European Union and its Member States"[70].

---

[65] EC Switzerland Free Trade Agreement 22 July 1972 official journal no. L 300, 31/12/1972 p. 0189
[66] 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland
[67] Directive 95/46/EC
[68] C-362/14 Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650 p.73
[69] 'Communication from the Commission to the European Parliament and the Council – Exchanging and protecting personal Data in a Globalised World' (European Commission 10 January 2017):http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN
[70] Ibid

To fulfil the requirements of being 'essentially equivalent', the Commission observes "the rule of law, respect for human rights and fundamental freedoms, relevant legislation...as well as the implementation of such legislation, data protection rules"[71] must be clear.

In Switzerland, the processing of personal data falls under the scope of the Federal Act on Data Protection[72] and its ordinances[73]. On the surface, these laws are quite substantial and, as the full title alludes to, are updated from the original 1992 law to reflect current matters. The last of these changes took effect on the 1st of January 2014, in what could be seen as a response to the drastic changes in the landscape of privacy that took place in 2013[74]. This law was viewed by the EU as strong enough to allow it to maintain its adequacy ruling as no investigation occurred.

Aside from simply having the legislation in place, the GDPR also requires a third country have "one or more independent supervisory authorities...with responsibility for ensuring and enforcing compliance with the data protection rules"[75]. For Switzerland, this is covered by the "Federal Data Protection and Information Commissioner" (FDPIC).

It is worthwhile to note here that Switzerland is also seeking to overhaul its own laws in this field. On the 15th of September 2017, the Swiss Federal Council published the long-awaited final draft of their proposal for a new Swiss Data Protection Act[76] that was duly sent to the Swiss Parliament for discussion; and can be expected to be implemented fully into Swiss law in the next couple of years.

This draft seeks to act in a manner to reflect the GDPR and act as a counterpart to the EU legislation, bringing around some important changes to the Swiss laws; including an improved transparency system under which data subjects will be informed of collection and processing; and improved breach notification mechanisms.

[71] GDPR Article 45(2)(a)
[72] Federal Act on Data Protection (FADP) of 19 June 1992 (Status as of 1 January 2014)
[73] Ordinance to the Federal Act on Data Protection. (FADP) of 19 June 1992 (Status as of 1 January 2014) and Ordinance on Data Protection Certification (DPCO) of 28 September 2007 (Status as of 1 April 2010)
[74] For example, the Snowden revelations
[75] GDPR Article 45(2)(b)
[76] "Die Sanktionen im Entwurf zur Totalrevision des Datenschutzgesetzes Datum": 15. September 2017

Of course, there are many other aspects to this law, which are highly like the GDPR, including impact assessments, privacy by design/default, rules on profiling, and an increase in criminal sanctions available. These same principles are also enshrined within the UK Data Protection Act of 2018 as it is an implementing act; so, the outcome of this and if the EU chooses to investigate could be a valuable insight for any future UK adequacy plans.

However, it is clear from the Swiss intentions, especially regarding their signing of documents[77] that, even if they wanted to take a different path, they are obligated to follow the European Union into a GDPR-esque system to ensure that they do not lose their largest trading partner.

This system is rather applicable to the UK's predicament, in terms of it overhauling its own privacy law, seeking a special relationship with the EU, and having its own air of independence as the Swiss do, while wanting to keep warm relations with its largest trading partner.

However, to keep as much, if not more, independence than the Swiss have with the EU, the UK would need to consider seeking adequacy in a similar vein to that of the Swiss.

5.1.3 Seeking adequacy for the UK

Of course, as part of this law and the Brexit negotiations, the topic of adequacy and the requirements has come up time and time again; with experts stating to the British Government that they will be "seeking unhindered data flows" and that they are "confident [that this will be] achieve[d]"[78]

[77] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108
[78] The Rt. Hon Matt Hancock, evidence to the EU Home Affairs Sub Committee, 1 February 2017, 11:02:35–11:03:03

Indeed, this came to the fore in mid-2017, when the House of Lords' European Union Committee published a report regarding the data protection implications in relation to Brexit[79]; this report was the result after calling for evidence from a plethora of individuals and experts and considering their views[80] . As expected, a lot of this report focused on ensuring "unhindered… [and]...uninterrupted"[81] data flows between the UK and EU post-Brexit. This was not only the view of the experts, but of the Committee itself[82], stating that it was a "consensus amongst our witnesses"[83] that securing adequacy from the Commission would be the most effective way of preserving data flows.

Such a report came to the relief of the incumbent Information Commissioner, Elizabeth Denham, who stated that "the UK has been so heavily integrated in the EU that it is difficult to say that the UK can get by without an adequacy decision"[84].

These strong opinions do raise the question of if the UK would be or could be successful should they choose to apply for an adequacy ruling from the European Union.

Firstly, as with Switzerland, the UK would need to show that it has "essentially equivalent" laws in place that are based on "the rule of law, respect for human rights and fundamental freedoms, relevant legislation...as well as the implementation of such legislation, data protection rules"[85].

The initial aspect of this is the relevant legislation and their implementation. As mentioned, the UK does have a recent Data Protection Act[86] in place, which follows the GDPR guidelines and

[79] House of Lords, 'Brexit: the EU data protection package' (parliament.uk 18 July 2017) <https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf
[80] ibid Appendix 2: List of witnesses
[81] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Rt Hon Matt Hancock MP, Minister of State for Digital and Culture' (parliament.uk meeting date 1 February 2017)
[82] House of Lords, 'Brexit: the EU data protection package' (parliament.uk 18 July 2017) para 110
[83] Ibid Para 111
[84] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (parliament.uk meeting date 8 March 2017)
[85] GDPR Article 45(2)(a)
[86] Data Protection Act 2018

uses it as a foundation[87]. While not a requirement of being an EU Member, Member States were encouraged to implement such acts into their national legislation to provide further clarification and to allow some deviation.

For the UK Act, they opted to deviate as much as feasibly possible from the original. Whilst keeping the heart of the GDPR in the law, largely due to the fact that, while in the EU, the GDPR will supersede the UK Law. However, the UK chose to take the option to change the age of children down from the default 16 of the GDPR[88] to 13 in its own law[89].

The UK have also used this act to further the powers of the Information Commissioner's Office, a right granted to them by the GDPR and one which proponents of the law sought to implement. The rationale behind this was that "extending the power of the Information Commissioner is interesting and sensible and could even be considered appropriate"[90], these powers are largely similar to the GDPR powers, but also allows the incumbent to refer to the Act when exercising powers, and clearly states the limitations of said powers[91].

These slight deviations should not concern UK legislators if adequacy is applied for, as it can be seen to be 'essentially equivalent' to the GDPR as they both use the same foundation, and the deviation of changing the age of a child to 13 is the same as implemented in many other EU Member States including Belgium, Finland, and Sweden. Indeed, the British Court of Justice has not considered "general compliance as a factor in the assessment of adequacy"[92]; this is also reflected in other adequacy decisions that have been granted to nations like Switzerland where the law may not be identical, but good enough.

The reasoning for this age differential seems to be to keep the law "in line with the minimum age set as a matter of contract by some of the most popular information society services which

[87] Ibid (Sections 1-3)
[88] GDPR Article 8(1)
[89] Data Protection Act 2018, Section 9
[90] HC Deb (15 May 2018) vol. 641, col. 177
[91] Data Protection Act 2018, Part 6
[92] Statement by Professor Ian Walden, EU Financial Affairs Sub-Committee, Uncorrected oral evidence: Data sharing post Brexit, Wednesday 23 May 2018 at approximately 10:40am

currently offer services to children"[93]. Key to this was the maintaining of relationships with "services which provide educational websites and research resources to complete their homework"[94].

Although one worrying aspect is that the UK may seek to make further changes and amendments to this Act at a later date as, during discussions, several high-ranking members of Parliament had issues with aspects of the GDPR entering into force within the UK. Included in these is the father of the House, Kenneth Clarke, who had clear problems with the "right to be forgotten"[95]. However, as it stands, no changes to this recent law have been mentioned or discussed within Parliament and therefore, this Act can be seen as being "essentially equivalent" as per GDPR guidelines; but the situation could change should pressure grow.

It is also worthwhile mentioning here that, should the UK apply for adequacy, the "practical effect of this is that the UK will need to accept the continuing influence (perhaps jurisdiction) of the CJEU over UK data protection law"[96]. This does not seem to deter the individuals within the British Brexit Committee, who recommended that they "would also have to accept the jurisdiction of the CJEU… [as it is] in the interests of the people and governments of Europe"[97]

The question about the UK successfully obtaining adequacy post-Brexit therefore is reliant upon other aspects of Article 45, namely "respect for human rights and fundamental freedoms"[98]. This could potentially be an obstacle for the UK's bid for adequacy due to several factors.

Firstly, in late 2016, the United Kingdom passed the Investigatory Powers Act[99], based on preventing terrorism despite no large-scale terrorist attacks happening in the United Kingdom

[93] Data Protection Act 2018: Explanatory Notes: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf
[94] Ibid
[95] Ministry of Justice, Lord Chancellor and Secretary of State for Justice, Rt Hon Kenneth Clarke MP, Speech at the British Chamber of Commerce in Brussels, 'Data protection', 26 May 2011
[96] B. Treacy, Expert Comment, Privacy & Data Protection Journal, 2018, 18(7), 2-3
[97] Exiting the EU Committee, 7th Report – The progress of the UK's negotiations on EU withdrawal: Data, HC 1317
[98] Article 45(1) GDPR
[99] Investigatory Powers Act 2016

that year[100]. This Act seeks to clarify the laws in relation to intercepting and storing communications and online activities of residents of the United Kingdom (including citizens from other EU Member States). It also details who can access the gathered data, including the British security agencies such as MI5 and MI6. The official stance of the United Kingdom government is that "it will provide unparalleled openness and transparency about our investigatory powers, create the strongest safeguards, and establish a rigorous oversight regime"[101]

The powers granted under this piece of legislation have drawn comparisons to the US Laws[102], comparisons that have led to widespread demonstrations and discussions amongst the populous of the United Kingdom in relation to the mass surveillance to which the Act enables. Many of these discussions arose in relation to the European Convention on Human Rights[103], especially Article 8[104] which calls for a right to privacy[105].

Previously, the European Union has ruled various sections of a similar Act to the Investigatory Powers Act[106] invalid based on this reasoning, this new Act is seen to have a much broader scope and some worry that the powers instilled here are far more reaching. There are challenges to be expected of this Act, but there are concerns that, should the UK split ties with the CJEU, such a case will not succeed.

[100] http://www.telegraph.co.uk/news/0/many-people-killed-terrorist-attacks-uk/
[101] Comment by Mrs Theresa May (Then known as The Secretary of State for the Home Department) HC Deb 15 March 2016, Column 773
[102] For example, Section 202 of the PATRIOT ACT
[103] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR) 1950
[104] Ibid Article 8: Right to respect for private and family life
[105] [2016] UKIP Trib 15_110-CH
[106] Data Retention and Investigatory Powers Act 2014 (Expired 31.12.2016)

In the past, there have been strong challenges to similar pieces of legislation in the United Kingdom, especially regarding DRIPA[107], the associated challenges[108]. Elsewhere, results have been positive for those who are concerned with privacy[109].

Currently, the Investigatory Powers Act will be declared invalid under European law unless rewrites are made to it; but the Act, even if defeated, will potentially arise again once European law no longer applies; the UK is seemingly performing a stalling tactic here to ensure the longevity of said Act.

This could be the largest obstacle for the UK obtaining adequacy. However, with France having similar legislation[110] in place, the UK could argue that such legislation is in line with EU Member standards and adequacy can be expected if argued in such a manner, provided there are no other objections.

Secondly, and further to the initial point, the British Government has clearly stated that "the Charter will not be converted into UK law by the Great Repeal Bill."[111] This could also factor into the right and respects element required for adequacy. The onus here is on the British government to provide a reasonable recourse for this, potentially using other legislation or case law as a foundation for these. This is further evidenced with the Government mentioning that "The Government's intention is that the removal of the Charter from UK law will not affect the substantive rights that individuals already benefit from in the UK"[112]

One cannot always guarantee something being a certainty though, so to call adequacy a foregone conclusion could come back to haunt individuals, despite experts stating that an "equivalence

[107] The Data Retention and Investigatory Powers Act 2014
[108] R. (on the application of Davis) v Secretary of State for the Home Department [2015] EWCA Civ 1185 (20 November 2015)
[109] Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Others [2016] UKIP Trib 15_110-CH
[110] Loi du 24 juillet 2015 relative au renseignement
[111] Department for Exiting the European Union, Legislating for the United Kingdom's Withdrawal from the European Union, Cm 9446, March 2017: [2.23]
[112] Ibid

determination…would be overwhelmingly the most likely outcome"[113]. Indeed, the Moroccan authorities apparently "submitted an adequacy request more than 12 years ago"[114] and have yet to be approved or even have an investigation conducted.

Of course, some have suggested that the UK may even be subject to a stricter review than other candidates prior to an adequacy ruling being granted, with experts commenting that "it is possible that post-Brexit, the UK would be held to a higher level of data protection"[115] and some political factors could weigh into the process.

To gain further insight into the potential of the UK obtaining adequacy, based purely on it being a 'third nation', and not in the context of a former member or mentioning the situation in other EU nations, it is worthwhile to see other countries which have been granted said status by the EU, how they obtained it, and what their future plans in this arena are.

5.1.4 Canadian System

Of course, with such an intrinsic network of data protection laws, the ability to grant adequacy status to other nations, and strong safeguards in place for personal data, Canada is one of the few nations that has been granted adequacy status. This status, however, extends only as far as commercial organisations by the European Union[116] due to PIPEDA[117] and was the first non-European nation to be given such a certification.

[113] Statement by Simon Gleeson, EU Financial Affairs Sub-Committee, Uncorrected oral evidence: Data sharing post Brexit, Wednesday 23 May 2018 at approximately 10:35am
[114] Statement by Professor Ian Walden, EU Financial Affairs Sub-Committee, Uncorrected oral evidence: Data sharing post Brexit, Wednesday 23 May 2018 at approximately 11:00am
[115] B. Treacy, Expert Comment, Privacy & Data Protection Journal 2018, 18(7), 2-3
[116] Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act
[117] Personal Information Protection and Electronic Documents Act, SC 2000, c 5

Canada is a nation that has close ties to both the EU, and the UK specifically, being a former British colony, a member of the Commonwealth of Nations, and sharing the same monarch.

Therefore, Canada serves as an important starting point in a UK assessment due to both holding a unique adequacy ruling, having a common law system in place, and a strong cultural link.

It is worthwhile pointing out here, that, while Canada is currently deemed adequate, the decision itself dates to 2001. The PIPEDA itself is of a similar age and, the main issue with the European Data Protection Directive[118] is apparent in the Canadian counterpart. The world, especially that of data, is drastically different from the world in 2001 and global attitudes are far beyond anyone's predictions. Technology has come so far in the last 17 years and has brought with it a mechanism for data to move around with such ease.

Initially, it has been said that "When the EU Commission originally gave Canada its adequacy, it was done so reluctantly"[119] and, as such, should attitudes change and the EU think more should be done, a review could see the first ever revocation of adequacy status. This would provide the EU with a bite to match the bark it produces about data protection standards and could signal a statement of intent.

Therefore, it does seem that if a review does happen, the odds do not fall in the favour of Canada. In the preamble of the GDPR, the European Commission has stated that the tests relating to adequacy now rely upon "essential equivalency"[120]. This could be where the ultimate downfall of the Canadian system occurs. Experts have identified several gaps between the Canadian law and the GDPR[121].

[118] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[119] https://iapp.org/news/a/could-canada-lose-its-adequacy-standing/ accessed 28.05.2018
[120] Recital 104 GDPR
[121] Examples of this is include not providing their Data Protection Authority the powers to make orders, no monetary penalties, rights for erasure and portability established

This may not be a worry for the United Kingdom, since they possess a recent data protection law that is designed to work in harmony with the GDPR. Unlike Canada, the UK also has a centralised Data Protection Authority in the form of the ICO; but as previously mentioned, there may be flaws with the British legal arena, and ICO may see its own role diminished.

Taking this view in a broader light, and importantly for the UK to observe, it reveals that the overall legal atmosphere in Canada may be an influencing factor. Indeed, the GDPR also makes overtures to "how a particular third country… [is built using] its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law"[122]. This could be cause for concern for Canada (and potentially the UK's application) for numerous reasons.

Primarily, Canada has become embroiled in surveillance discussions due to their membership of the controversial five eyes network (along with the United Kingdom) which embarked in spying operations on foreign citizens and openly shared their results with select nations.

EU law provides for the Commission to conduct such a review at regular intervals[123], but not confirming what this entails. However, with Canada and the EU passing the "Comprehensive Economic and Trade Agreement"[124], and agreement approved by all Member States following two years of negotiations and seven years of planning; it is likely that if EU Member States had issues with Canadian data protection law at this point for trade, the topic would have come up.

While a review could happen, and the result likely to be the stripping of adequacy, it could be seen that this hesitancy to conduct such a review stems largely from the EU seeking to avoid more data controversies in third countries, following the debacle of the Safe Harbour rulings, Privacy Shield challenges, and Snowden revelations.

[122] Recital 104 GDPR
[123] Article 45 GDPR
[124] Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part

This could be some relief to the UK who may adopt a similar approach, especially with the necessity of data flows being open on both sides of the English Channel being a key importance to both the EU and the UK. This, coupled with the likelihood that both sides will seek some sort of trade deal, potentially in a similar vein to the Canada one, means that a direct review could be unlikely, despite one being needed every 4 years under the GDPR[125].

The UK could skirt around the subject of a review for a potentially indefinite period and therefore maintain an adequacy ruling but be teetering on the precipice of losing it should relations with the EU further sour.

Of course, a review could still happen much in the same way the Safe Harbour ruling came about, namely a legal challenge over a Canadian company. While there are no tech titans the size of Facebook and Google who call Canada their home, the target to strike is not as clear as that of the United States, especially when comparing an adequacy ruling with the Privacy Shield.

This challenge could happen against a UK company though, with more of the larger businesses who intertwine their operations in the EU based in the UK, such as in the financial and technology sectors. This could be a cause for concern should the UK apply in a similar vein to Canada and opt to only have adequacy for certain sectors; while this is unlikely as the UK will most likely aim for an adequacy ruling which provides blanket coverage, it could still be a possibility.

However, while the danger of a review remains for Canada, privacy enthusiasts are pushing for an updated law to ensure that, should a review happen, Canada's status as an EU data partner is maintained. Indeed, in the spring of 2017, the Canadian House of Commons did conduct their own review of the PIPEDA through the eyes of the GDPR[126] and if Canadians should be concerned about losing such a status; and, if lost, how consequential it would be. This review

[125] Article 45(3) GDPR
[126] Standing Committee on Access to Information, Privacy and Ethics (ETHI) 42nd Parliament, 1st Session Meeting No. 52 Tuesday, March 21, 2017, 3:30 p.m. to 5:30 p.m.

does act as a good guideline as to what the UK could expect to see if they cannot have adequacy status.

The conclusion of such a review found that views were divided. Of course, there was an agreement that there would be "a cost if...a country like Canada, a trade partner, were to lose its adequacy status"[127]. Conversely, others warned about this being an obsession and to not let this seeking of approval from the EU detract from the underlying message of providing a good balance between promoting business needs and having protection for personal data. Indeed, one of the experts in the review mentioned that this adequacy decision was simply a "symbolic message that Canada was a safe jurisdiction within which personal data could be processed [but instead Canada should]…modernize PIPEDA because it needs modernization, not because it will satisfy a vague and shifting set of standards imposed from Brussels. We should take note of what the Europeans have done and draw lessons"[128]

It is worthwhile to mention here that, much like the EU (and the UK), different sections of Canada can enact their own, independent laws. One such province, Quebec, did seek its own adequacy before the GDPR and the EU assessed Quebecois law and rejected said application, dressing it down in an Article 29 Working Party Paper[129]. This is crucial as it could paint a picture as to what would happen should Canada lose adequacy. It is unlikely that any province individually could attain adequacy under current laws. This could serve as an obstacle if the British territories, including Scotland, find themselves stripped of adequacy, although this topic has yet to be brought up by the European Commission.

While studies have not yet assessed if Canadian companies have gained an advantage in an economic sense from the current adequacy ruling, comparisons can be drawn from Canada's southern neighbour as to what a controversial data-sharing situation can mean. The United States

[127] Ibid, Prof.C.Bennett at 17:05
[128] Ibid
[129] Article 29 Working Party: 'Opinion 7/2014 on the protection of personal data in Quebec ' (WP219, 4th June 2014)

remains the EU's largest trading partner[130] and there are no studies that can show companies have opted to locate in Canada purely due to the adequacy status.

Applying this to the United Kingdom, worries have been expressed that businesses could relocate themselves to an array of EU cities to keep up with demand, suggesting Dublin for technology, Frankfurt for finance, and the Nordic nations for start-ups. The data from Canada is a good sign for the British economy in this regard, as the impact is expected to be minimal, especially if adequacy is obtained in even one of these areas. Contrary to this, experts have suggested that if the UK were to not have an adequacy ruling and operate under a different system, it may convince firms that it is more cost-effective and less cumbersome to host data in the EU rather than the UK[131]

However, it is worthwhile to remember that adequacy does not guarantee a strong economy, and a lack of adequacy does not condemn a nation. Alternative transfer mechanisms do exist which would most likely come to the fore should Canada (and extrapolated to a UK scenario) lose adequacy status. A similar protocol was used following the invalidity declaration of the Safe Harbour, with many companies opting for model clauses in the interim and continuing with such clauses despite the Privacy Shield. These will be discussed in further detail further on.

Further to this, and using trading partner sizes as a base, the largest Canadian trading partner within the EU is the United Kingdom. Canada has already made it clear that, in addition to the EU free trade agreement in place, they would actively pursue an agreement with the UK for free trade after Brexit[132] which could, potentially, include the declaration of adequacy of data protection standards between the nation which would severely assist the UK's application for EU adequacy.

[130] 2017 report by Directorate General for Trade: http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.04.2018.pdf
[131] Phil Muncaster, 'Global Firms Could Pull Data Out of Post-Brexit UK', 5 July 2016 accessed 28.08.2018
[132] Statement by Canadian Prime Minister Justin Trudeau on 11.04.2018

5.1.5 Japan's Adequacy: A guide for the UK

In terms of modern adequacy status, the most recent of these nations to be declared adequate under the GDPR by the EU is Japan, reaching this status in mid-2018. This is important to evaluate for the UK as both the UK and Japanese laws are recent and reflect the change in the global scheme of privacy; it also highlights the route to adequacy as painted under the new, GDPR-focussed European Commission.

In a statement from the EU commission at the end of May[133], both Japan and the EU "reaffirmed that a simultaneous finding of an adequate level of protection by both sides will complement and enhance the benefits of the Economic Partnership Agreement between Japan and the EU, which is currently proceeding for the signing, and that the finding will also contribute to the strategic partnership between Japan and the EU"[134].

Once more, extrapolating this to a UK scenario, the EU will highly value having such a deal in place in the event of a softer Brexit, if there is already some form of Economic Partnership Agreement in place.

However, it must be noted that, despite these somewhat shared views of data protection between the EU (and therefore the UK) and Japan, there are key differences between the privacy laws, even after the Japanese reforms.

One such example of this is the establishment of a "Personal Information Protection Commission" (PIPC) under the Japanese law. This commission works in a somewhat similar vein to the EU Data Protection Authorities, but it has the sole focus of establishing and enforcing privacy regulations, which may provide a further reach than individual EU Data Protection Authorities, or even the EU Data Advisory Board established under the GDPR[135].

[133] Statement/18/402, Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection on the state of play of the dialogue on data protection Tokyo, 31 May 2018
[134] Ibid
[135] GDPR, Article 68

However, in recent months, much has been done to improve and speed up this process. The governments of both the EU and Japan have agreed "on solutions to bridge relevant differences between the two systems"[136]. This does imply that changes are being performed by both the EU and Japan to find an adequate middle ground.

This is a positive sign for the potential British application as it shows, unlike with the Brexit negotiations, the EU is somewhat willing to be flexible when assessing a nation's data framework. Leading to the previously raised issues such as surveillance and human rights potentially overlooked to focus on the greater good of having such an agreement in place.

While nothing has specifically been made public, the statement[137] does allude to the Personal Information Protection Commission adopting Supplementary Rules and the European Commission clarifying "the legal nature and effect of the [GDPR] in the European Economic Area"[138]

5.1.6 Adequacy Plus

It must be said though, especially using Miss Denham's remarks[139] as a base, that adequacy could be the minimum of expectations. The idea of something further than adequacy, an 'adequacy plus'[140] is an idea which has been mooted on occasion[141]. Indeed, this speech touched on the valid concept that something beyond a 'traditional' adequacy decision is something that

[136] Statement/18/402, Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection on the state of play of the dialogue on data protection Tokyo, 31 May 2018
[137] Ibid
[138] Ibid
[139] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (parliament.uk meeting date 8 March 2017)
[140] Rezzan Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)
[141] For example PM speech on our future economic partnership with the European Union' (GOV.UK 2 March 2018)

the UK will seek, to pay respect to the long and intertwined trading links between the United Kingdom and the European Union once the UK does leave.

A key part of this is the role of the Information Commissioner's Office (ICO), the aforementioned Data Protection Authority of the United Kingdom. This is evident with the British Prime Minister hoping that Brexit negotiations will result in "an appropriate ongoing role for the UK's Information Commissioner's Office"[142], a role that would potentially allow UK businesses to be included within the so-called "one-stop-shop"[143] regime. Quite simply, this system is constructed around the ideals of the GDPR and harmonisation of laws and authorities.

This "one-stop-shop" inclusion would allow businesses and companies located within multiple Member States are only required to report to one authority[144]. Inclusion in such a scheme is imperative for businesses based in the United Kingdom if they wish for a more streamlined process for compliance matters. Indeed, should the UK be excluded from such a scheme, businesses based within the UK would be forced to interact with the supervisory authorities within each nation they operate in[145], potentially meaning 27 differing interactions either directly or with a representative[146].

Membership into the "one-stop-shop", of course, would be highly preferable for British businesses and a strong deciding factor when companies are choosing where to base their operations; a view that both the Information Commissioner[147] and the Prime Minister[148] share. The advantage of this would be maintaining some degree of harmony between the British and

[142] 'PM speech on our future economic partnership with the European Union' (GOV.UK 2 March 2018)
[143] GDPR Article 60 and Recital 127
[144] Current guidelines have this as where the business has its main European establishment or Data Protection expertise
[145] Based on Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (European Commission 5 April 2017)
[146] GDPR Article 27
[147] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (parliament.uk meeting date 8 March 2017)
[148] 'PM speech on our future economic partnership with the European Union' (GOV.UK 2 March 2018)

European frameworks, causing low levels of disruptions which could be seen as being on par with EEA membership in that regard.

Beyond this, the influence of the ICO within the European sphere is something which is being used as a bargaining chip when discussing this potential 'adequacy plus'. Under its current guise, the ICO is viewed by many as a guiding voice of data protection issues within Europe[149]. Be that through providing detailed GDPR guidance, being active and vocal about ongoing investigations[150], or the fact that the ICO has a large say in the actual text of the GDPR. The ICO is a key figure; and part of a data protection relationship in Europe which both parties would ideally like to see continue.

While it must be said that "the adequacy-plus aim is certainly bold and ambitious"[151], the provisions of the Data Protection Act[152] do provide the UK with a good springboard into such a scheme, even if the actual status of the UK is not known until well beyond Brexit itself and it will be largely the decision of the European Commission.

However, the signs from the EU do look promising as the Commission has endorsed proposals that as "the protection of personal data is a fundamental right in the EU, it cannot be subject to negotiations in the context of EU trade agreements"[153]. In layman's terms, this could be interpreted as the EU not wanting to discuss this issue within the context of Brexit negotiations, which have been heated at times and instead taking the stance that that the "preferred avenue for the EU are 'adequacy decisions'"[154] and that there is limited room for manoeuvre within the GDPR.

[149] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Antony Walker, Deputy CEO, techUK; Ruth Boardman, Co-Head, International Data Protection Practice, Bird and Bird' (parliament.uk meeting date 1 February 2017)
[150] For example, the ICO is very public about the current Cambridge Analytica investigation
[151] Rezzan Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)
[152] Data Protection Act 2018
[153] 'College Meeting: European Commission endorses provisions for data flows and data protection in EU trade agreements' (European Commission 31 January 2018)
[154] 'College Meeting: European Commission endorses provisions for data flows and data protection in EU trade agreements' (European Commission 31 January 2018)

This view is echoed by the British government who have also stated a similar point that "while there are signs that the EU is moving to the inclusion of data in trade agreements, the current pattern appears to be for a trade agreement to be negotiated separately and in parallel to the process of an adequacy decision"[155].

The obvious drawback with this is the fact that the UK could disregard other options in order to focus on obtaining 'adequacy plus', which could ultimately fail and lead to there not being a safety net in place should things go awry. This is a highly dangerous tactic to have in place, especially with the EU seemingly holding all of the cards for this negotiation.

It is important to mention here that, despite using other countries as a basis for predicting a potential soft-Brexit deal for the UK, this is unchartered territory. Never has a Member State left the EU or even come close to leaving; only three former territories of EU Member States have left (Algeria, Greenland, and Saint Barthelemy). Even in this case, Greenland made it a priority to maintain a good trading relationship due to its close ties with Denmark[156].

On the topic of unchartered territory, if the UK were to obtain an 'adequacy plus' ruling, there is no saying as to what this will ultimately mean. While overtures have been made as to some aspects of it, it is still unclear what elements it will have and how far such a ruling will extend.

These options presented, be they EFTA or EEA membership, pushing for immediate adequacy, or even aiming hiring for an 'adequacy plus' agreement could all still conceivably be on the table with the right work performed by both negotiating parties. The issue is the sheer stubbornness of the parties and the pressure applied to them behind the scenes to not yield any ground to the other with negotiations.

[155] Exiting the EU Committee, 7th Report – The progress of the UK's negotiations on EU withdrawal: Data, HC 1317

[156] Greenland does remain subject to the EU treaties through association of Overseas Countries and Territories with the EU via the 'Greenland Treaty'.

While much can be inferred from these potential options, there could be other deals which can be struck as part of a soft Brexit, which appeals to the special status the UK holds, ones which could not be comprehended at this moment in time, but still could come to the fore before the deadline strikes.

5.2 Hard Brexit

Of course, the other side of the proverbial Brexit coin is the concept of a ‘Hard Brexit’. This is the scenario wherein the UK leaves the EU without any sort of deal in place, essentially reverting all laws and agreements back to before the UK joined. This is defined by an exit from the EU’s Single Market and EU Customs Union, and a refusal to recognise the European Court of Justice’s (ECJ) authority. This would mean that the UK would fall back to the World Trade Organisation’s standard rules and be expected to build up from there.

As previously mentioned, this option is still on the table and, as of October 2018, it appears to be the direction negotiations are heading, with the UK and EU both holding firm in their stances in an effort to gain the upper hand.

5.2.1 Initial happenings

The concept of the ‘cliff edge’ is something that is looming as a reality. If such an event does occur, aside from the pandemonium that would sprout up in the various other sectors of the relationship, be that trade, travel, finance, or the plethora of others, the field of data protection is also due to experience a seismic shift.

As midnight passes, and the UK falls off the proverbial cliff edge, the data flows between the EU and the UK will largely become illegal and declared unsafe unless a deal is in place. While it is likely that many businesses will have enacted other safeguards to transfer, as discussed below, there will remain a large number who inadvertently find themselves operating with illegal data transfers either due to not understanding the events correctly, believing the rules will not apply to them, or simply forgetting that such a system is in place.

In the period between the cliff edge and guidance from either the Commission or ICO itself, a great deal of danger could arise, despite the UK still technically operating under its own act and protecting data to an equivalent standard as the EU. This technicality is where the issue arises, and businesses will need to assess how best to solve this in the quickest amount of time.

Parallels with this could be drawn with how non-EU businesses worked with the GDPR. While most continued unhindered, several high-profile companies instead simply turned data flows off to their companies from the EU, including American news sites such as the Chicago Tribune and the Los Angeles Times[157]; British businesses may do likewise for EU users to further protect themselves.

5.2.2 Removal of adequacy for UK's associated territories

As mentioned earlier, there are several overseas territories of the UK which are in possession of an adequacy decision based on their laws and categorised as being "closely integrated with the European Union and its Member States"[158] (These are Guernsey[159], Jersey[160], and the Isle of Man[161]).

Due to their close connection to the UK, but without following the same laws, many British and international[162] businesses have relocated to these territories for taxation purposes, as they can be considered "tax havens" by some[163]. Therefore, the retention of adequacy is a key element for the survival of these territories.

Indeed, adequacy was so key for Guernsey that it was one of the first locations to overhaul its own privacy laws to complement the GDPR, expressing this commitment within months of the

[157] https://www.nbcnews.com/tech/tech-news/chicago-tribune-los-angeles-times-block-european-users-due-gdpr-n877591
[158] 'Communication from the Commission to the European Parliament and the Council – Exchanging and protecting personal Data in a Globalised World' (European Commission 10 January 2017): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN
[159] 2003/821/EC: Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (Text with EEA relevance) (notified under document number C(2003) 4309)
[160] 2008/393/EC: Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (notified under document number C(2008) 1746) (Text with EEA relevance)
[161] 2004/411/EC:Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man
[162] For example: Apple Inc relocated it subsidiary to Jersey from Ireland for tax purposes
[163] https://www.theguardian.com/business/2007/nov/04/4

GDPR's text being finalised[164], stating that they considered access to the EU single market as "crucial"[165].

The fortunate news for these overseas territories is that their status as adequate nations will not be affected regardless of the state of Brexit as the GDPR does state that adequacy decisions from the previous Directive[166] "shall remain in force until amended, replaced or repealed"[167]. Of course, there is still the provision in the GDPR that states that there will be a "periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation"[168].

Key to this is the mention of "relevant developments"; this is a rather ambiguous term which could, if viewed through a specific lens, include the territory's relationship with a fully-fledged third country without an adequacy decision, which may well be the United Kingdom should a hard Brexit occur. The EU have shown previously that onward transfers from an adequate nation to a non-adequate nation is a sticking point for their rulings.

This could theoretically spell either the end of data flows between the territory and the EU, or between the territory and the UK. The decision may befall the government of each of the three territories as to which relationship is more valuable to them, or if a workaround can be found.

5.2.3 Reliance upon other systems

Aside from the territories, should such a fate befall the British mainland, and a hard-Brexit turns into a reality, British businesses may find themselves looking down other avenues to ensure a continued relationship with the EU and its residents.

[164] General Data Protection Regulation' (gov.gg 16 September 2016): http://www.gov.gg/gdprnews
[165] Ibid
[166] Directive 95/46/EC
[167] GDPR Article 45(9)
[168] GDPR Article 45(3)

While the GDPR does provide the possibility of some mechanisms for this to continue (to be discussed later), there are a couple of other systems adopted by non-EU 'third countries', such as the United States; a highly important trading partner for not only the United Kingdom, but the European Union as a whole.

5.2.4 The US model: Safe Harbour and Privacy Shield

It has been suggested that if a Hard Brexit occurs and, for some reason, the UK is not granted adequacy, either immediately or at all, the option to mirror the agreement the United States has with the EU could be applied. Despite the strong data protection framework, the United States does not have an adequacy ruling, nor has it officially applied for one.

This lack of adequacy status could be due to the EU and the US having opposing attitudes when it comes to the protection of personal data. Whilst the view of the EU has been well documented within this paper, on the other side of the Atlantic, personal data is seen more as a currency, wherein individuals can pay for services with their personal data, therefore losing it to the companies they offer it up to. This is perhaps best demonstrated with companies such as Facebook and Google offering services for free, but utilising their customer database to sell advertising space.

This led to the scenario wherein data transfers from the EU to the United States were governed by the "Safe Harbour" principle[169]. This method relied upon a promise from the government of the United States that all data transferred from the EU would be afforded a higher level of protection than originally provided under the laws of the United States. To qualify for the scheme, a company based in the US could self-certify with the Department of Commerce on an annual basis. Stating that it had complied with seven basic principles and other similar requirements that supposedly equated to meeting the data privacy adequacy standard of the EU. This principle was a pivotal aspect of international data transfers largely due to the somewhat

[169] U.S. Department of Commerce, Safe Harbor Privacy Principles and Related Frequently Asked Questions, July 21, 2000

complex relationship between the EU and the US, especially amongst some key sectors such as social media, finance, and technology and the speed in which companies could sign up for the scheme was to be of a great benefit to the ease of conducting business.

However, the Safe Harbour principle was not without critics or challenges towards the effectiveness, legality, and validity of the scheme. These were largely borne out of the fact that many US-based organisations, popular with EU citizens such as Instagram and Wikipedia avoided compliance with the scheme while still joining[170]. In tandem with this, the original Safe Harbour scheme was not applicable to key services such as airlines, banks, and telecommunications providers[171].

Further critiques appeared shortly after the leaks made public by the Snowden revelations, detailing how "the law and practice of the United States... [did not offer] sufficient protection against surveillance by the public authorities"[172]. One of the key challenges borne out of these revelations was the case of Schrems[173]. This case evolved from a complaint to the Irish Data Protection Authority by Maximillian Schrems, an Austrian privacy enthusiast, regarding the transfer of some of his personal data by Facebook from their EU servers in Ireland to the United States. The Irish authority initially dismissed his complaint, clarifying that it had no standing to act upon his complaint since Facebook followed to the Safe Harbour Agreement and the Irish authority was therefore bound by the European Commission's decision that recognised that Safe Harbour provided an "adequate level of protection"[174].

However, upon request by the Irish High Court, the CJEU discussed as to whether the Irish authority could indeed investigate Facebook's data protection practices to see if they were indeed

[170] T. Katulić, From Safe Harbour to European Data Protection Reform, MIPRO 2016/ISS
[171] C.Connoly, EU/US Safe Harbour – Effectiveness of the Framework in Relation to National Security Surveillance, Galexia, Speaking / background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on "Electronic mass surveillance of EU citizens", Strasbourg, October 7 2013
[172] EU Press Release No 117/15
[173] Case C-362/14 Maximillian Schrems v Data Protection Commissioner
[174] Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000

adequate or whether the Irish authority had to defer this responsibility to the European Commission's earlier approval of the Safe Harbour framework.

On the 6th of October 2015, the CJEU did rule on this. The first ruling arising from this was that the CJEU clarified that, regardless of the Commission's Decision on the Safe Harbour agreement, national supervisory authorities do not have their powers reduced. Indeed, they stated that national Data Protection Authorities "must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him"[175].

This further led to the CJEU officially declaring the Safe Harbour principle invalid, utilising Article 25 of the Data Protection Directive to justify themselves as the Commission are bound to examine any domestic laws or international agreements of non-EU nations ahead of declaring adequacy, a trait which has been carried through into the GDPR. As the original 2000 declaration did not have any findings in this vein, the 2000 decision was invalid.

The outcome of the Schrems case therefore was overwhelmingly successful for Mr. Schrems and proved to be the final nail in the coffin for this scheme.

Therefore, the UK would be ill advised to follow a similar scheme of self-certification akin to the Safe Harbour principle, even with the necessary authority in place and a stronger data protection law. Simply put, having businesses self-reporting and promising to uphold the standards required in a foreign territory is not a technique that can be used in the new GDPR landscape.

However, much like the UK, the importance of data transfers between the US and the EU cannot be understated. This a view shared by the governments of both the US and the EU who ensured during the Schrems[176] case that a secondary process was in place to act as a safety net should the decision result in the demolition of the Sage Harbour principle. The purpose of this was "to

[175]Case C-362/14 Maximillian Schrems v Data Protection Commissioner, para 99
[176] Ibid

avoid a potential cliff edge moment"[177]. This resulted in the Privacy Shield process, which meant the cliff edge was not realised.

Under the Privacy Shield, companies based within the US are required to sign an agreement and pass stringent tests to show they are compliant with EU data protection standards (the GDPR post-25th May 2018) which operate under monumentally higher standards than those under the US laws. On the surface, this system runs similarly to the Safe Harbour principle, but requires companies to sign up and opt in to the scheme instead of it automatically applying to them.

The similarities of the Privacy Shield also extend to some of the issues raised in Safe Harbour cases, including lax checks and regulations for firms, and a clear lack of information provided by the US government to their own companies. This, in essence, could cause the Privacy Shield to be seen as the same as the Safe Harbour principle, but with a new coat on it. There is not much information as to companies failing the Privacy Shield test or being reviewed by the United States' authorities on the matter.

In tandem with this, the United States have made assurances regarding their surveillance activities, especially in relation to EU citizen data[178], which is a key concern raised by the GDPR. Of course, these assurances require a great deal of trust, which may be waning, especially under the Trump administration which has adopted an "America First"[179] rationale, promoting American interests above all else. This had led to legal action being taken against the Privacy Shield by the same parties who overturned the Safe Harbour principle[180] and, despite initial setbacks, more are challenges are expected.

[177] Statement by Professor Ian Walden, EU Financial Affairs Sub-Committee, Uncorrected oral evidence: Data sharing post Brexit, Wednesday 23 May 2018 at approximately 10:30am
[178] European Commission - Press release: "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield Strasbourg, 2 February 2016"
[179] B. Katulis: "Democrats Need a Strong Alternative to Trump's 'Economic Nationalism'": https://foreignpolicy.com/2017/03/17/democrats-need-a-strong-alternative-to-trumps-economic-nationalism/
[180] Digital Rights Ireland v Commission, T-670/16

5.2.5 Potential Suspension of Privacy Shield

One such challenge, which looks likely to succeed in some form or another, comes from within the EU itself with the call to suspend the Privacy Shield[181] if the United States do not comply by the standards they promised to by the 1st of September 2018. Indeed, the Civil Liberties Committee (LIBE) made this an official ruling and not just a statement by passing a resolution stating that the agreement does not adequately protect privacy[182]. While the September deadline has passed, the situation is due to be reviewed in full by the EU during October, with the stance of LIBE clear.

A lot of this concern stems from the limited response by the US authorities to the Cambridge Analytica breach and the CLOUD Act[183], which would severely undermine the work and scope of the GDPR along with the failure of the American administration to appoint a permanent privacy ombudsman.

In layman's terms, the CLOUD Act behaves as an update to a series of former US Laws[184] from 1986 which regulated how United States law enforcement officials can access data stored outside of the United States.

The crux of this legal update is the removal of the Mutual legal-assistance treaty (MLAT) barrier for enforcement. Under the old laws[185], the US could only gain access to overseas data through MLATs. This was a lengthy process, requiring the nations involved to write down the details of the assistance with legal investigations before going to a vote in the US Senate; a notoriously tricky collective dependent upon the political climate.

[181] http://www.europarl.europa.eu/news/en/press-room/20180611IPR05527/eu-us-privacy-shield-data-exchange-deal-us-must-comply-by-1-september-say-meps accessed 18.06.2018
[182]Draft motion for a resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-U.S. Privacy Shield (2018/2645(RSP))
[183] United States Clarifying Lawful Overseas Use of Data Act 2018
[184] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.
[185] Ibid

Under the CLOUD system, US law enforcement officials (ranging from local police officers to federal agents) can force technology companies to turn over user data, regardless of where said data is stored, even if it is in the EU.

Another addition to this law is the ability for the executive branch (The President of the United States) to enter into what is referred to as "executive agreements"[186], allowing the incumbent in the Oval Office to agree with other nations to share all data regardless of the host nation's laws or congressional approval. This, again, could see the United States forwarding EU citizen data to other nations if the executive branch decides to do so.

It remains to be seen how this potential suspension will play out, whether the US will comply with the order, whether the EU will not back the resolution, or whether the Privacy Shield will suffer the same fate as the Safe Harbour.

However, if suspension does occur, some can expect US businesses to adopt a similar approach to that of the Safe Harbour being invalidated. When this happened, "many US companies…had sent to every customer the standard contractual clauses that are the alternative to an adequacy decision"[187] within 12 hours of the ruling.

However, regardless of how this turns out, the sheer fact that the overarching method of transfers to the United States has come under recurring fire from privacy advocates within the EU should be somewhat alarming for the UK should a Hard Brexit occur. This is especially important if those in power opt to follow a more US approach to data flows, using the importance of said flows as a bargaining tool with the EU.

While the same concerns with the US are visible in the UK regarding surveillance and the ability to override the law for certain groups, the foundations of the British law could be seen as being stronger, especially if the Investigatory Powers Act is fully declared invalid by the courts.

[186] United States Clarifying Lawful Overseas Use of Data Act 2018, Section 4(9)
[187] Statement by Professor Ian Walden, EU Financial Affairs Sub-Committee, Uncorrected oral evidence: Data sharing post Brexit, Wednesday 23 May 2018 at approximately 10:30am

5.3 GDPR transfer mechanisms for Third Countries

Aside from this system, there exists a few mechanisms detailed within the GDPR which have become established options for businesses operating in nations which are not deemed adequate or could run into trouble with either their adequacy decision (such as Canada) or their method of transfer (such as the United States).

It is important to stress here that these mechanisms are not immediately applicable and cannot simply be called upon; they can also only be used on a business-by-business basis, and not instantly put in place for all businesses with a click of the fingers. They require preparation work, a commitment, and, in some cases, a requirement to be thoroughly vetted by a respected body.

5.3.1 Model Clauses

One system that has been utilised in countries that are not considered adequate, or have issues ascertaining to data protection is the concept of 'model clauses', otherwise known as 'standard contractual clauses'. These mechanisms were enabled under the previous directive[188] to allow controllers within the EEA to transfer personal data to 'third nations'.

The crux of this mechanism is that obligations for protection of said personal data are placed on both the sender and receiver of the data. This is to ensure the 'rights and freedoms' of the data subject are always protected; this is done through inserting clauses into contracts between the parties, or even drafting separate agreements solely for this purpose if the agreement predates the use of these clauses.

Model clauses can be seen as highly advantageous for businesses who wish to conduct trade quickly and efficiently with other businesses with minimal disruption. While carrying more weight to them than a simple promise, these clauses work along a similar vein to that of the

[188] Directive 95/46/EC

previously discussed American mechanisms, therefore bringing with them the same critiques that accompany such a system.

These clauses are set to remain applicable under the GDPR, and newer versions are aiming to tackle some of the concepts brought in by the Regulation, such as for joint controller[189] and the new responsibilities placed upon processors[190].

Guidance in this field for a post-Brexit world has been made available by the EU for this exact matter[191]. The fortunate aspect of this report, from a UK perspective, is the EU essentially committing to the fact that these clauses will remain valid and available unless the Commission rescinds them. Therefore, these clauses are free for use by UK businesses who wish to trade with the EU post-Brexit in the event of a hard Brexit. Indeed, the Information Commissioner has stated that the clauses are "probably the mechanism that a lot of particularly small and medium businesses would use in this scenario."[192]

The important caveat here is to mention of the potential rescindment of this mechanism. As mentioned earlier, the challenge by Schrems to the Safe Harbour principle[193] and further challenges to the Privacy Shield[194] could lead to a knock-on effect which could make the entire concept of model clauses invalid, and therefore rescinded by the Commission.

This is already in the process of happening, based on the fallout of the Safe Harbour and challenges in the Irish courts in relation to Facebook's reliance on the model clauses as a backup mechanism. The challenge from this was that this mechanism did not have the same safeguards as could be expected from an adequate nation and a severe lack of legal redress, which is required to ensure the rights and freedoms of data subjects.

---

[189] GDPR Article 26
[190] GDPR Articles 28 and 29
[191] , 'Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection' (European Commission 09 January 2018): http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245
[192] Statement by Elizabeth Denham, Exiting the EU Committee, 7th Report – The progress of the UK's negotiations on EU withdrawal: Data, HC 1317
[193] C-362/14 Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650
[194] C-498/16 Maximilian Schrems v Facebook Ireland Limited [2018] ECLI:EU:C:2018:37

In the courts, the topic of the American protection standards were brought into the limelight. Once more, the topic revolved around the issue of American surveillance, where it was stated that personal data "is wrongly interfered with by the intelligence services of the United States"[195] and that the "issue of the validity of the SCC [standard contractual clauses] decisions [should be referred] to the CJEU for a preliminary ruling"[196].

Once more, the UK should be paying attention to these developments as, from a surveillance angle, the British government finds themselves in the same boat as the Americans. The British surveillance infrastructure is akin to the American one, and, even if the model clauses system is only declared invalid for the US, the UK could also be challenged on a similar footing.

As of August 2018, this matter is yet to be considered by the CJEU, but it is clear based on the Privacy Shield issues, that this is a topic the CJEU will take very seriously and their answer could result in personal data transfers to the US under this clause mechanism to be invalid.

For now, the implications of the rescindment of model clauses for the UK in a post-Brexit world is unclear, but certainly something which should be considered by businesses on both sides of the English Channel who wish to conduct trade with one another.

5.3.2 Binding Corporate Rules

Another, perhaps more stable, mechanism that would be available to businesses wishing to operate on both sides of the English Channel in a post-hard Brexit world would be that of Binding Corporate Rules (BCRs). This mechanism is designed for global companies who wish to operate both inside and outside of EU borders; and companies such as Airbus, Accenture, and eBay are companies who have utilised this system[197].

[195] Data Protection Commissioner v Facebook Ireland Limited and another [2017] IEHC 545 p. 339
[196] Data Protection Commissioner v Facebook Ireland Limited and another [2017] IEHC 545 p. 340
[197] http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50116

This mechanism has been made available to businesses since 2003[198], through the Article 29 Working Party and using the previous law[199] for guidance. The rationale behind the creation of BCRs seems to stem from two main issues with the prior mechanism of model clauses. These are that they "prevent a Member State from determining that a data exporter ready to enter into a contract in line with the standard contractual clauses does not offer sufficient safeguards for the transfer to take place"[200] and that there is an issue regarding "onward transfers to other recipients different from the data importer"[201].

At their core, BCRs allow the construction of a system within a company to allow the free flow of data, treating all corporate offices as based within the EU, even if this is not the case. Of course, the system for building a BCR framework is neither easy nor simple, it is highly complex, featuring a plethora of proverbial hoops to jump through which "can take two to three years to get through"[202], and a commitment to monitoring compliance and constant communication with a designated lead authority. This could serve as an issue if British businesses are just starting to consider such an option, as they may need to rely upon another mechanism in the meantime if a hard Brexit does happen.

It is also worthwhile mentioning here that the application and implementation process to obtain a BCR is convoluted and varies between nations, depending upon whom is selected to be the lead authority for a business.

[198] Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (European Commission 3 June 2003): http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf
[199] Directive 95/46/EC
[200]Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (European Commission 3 June 2003): http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf
[201] Ibid
[202] Statement by Rosemary Jay, EU Financial Affairs Sub-Committee, Uncorrected oral evidence: Data sharing post Brexit, Wednesday 23 May 2018 at approximately 10:40am

This, of course, is compounded by the fact that BCRs have been commuted over from the Data Protection Directive and into the GDPR as a mechanism for international data transfers[203]; and that existing BCRs granted under the Data Protection Directive can still be relied upon under the new Regulation.

What this means is that each set of BCRs needs to designate one EU Data Protection Authority to whom they report to, and who they are accountable towards, as per the GDPR[204], much in the same way EU businesses are required to nominate one too[205]. BCRs would, in this sense, work in a similar vein for individual UK businesses as the aforementioned "one stop shop" mechanism discussed in the soft-Brexit section of this paper.

Of course, there are drawbacks for if a business chooses to solely rely upon BCRs, the largest of which is that only 19 Member States currently utilise the method of mutual recognition for BCRs. This would mean that, if one of the 19 approves a BCR application, the others "have confidence in their decision and accept their findings without further scrutiny or comment"[206].

Whilst this could be good for the United Kingdom as they find themselves within this group of 19 nations (and are the lead authority for around a quarter of BCRs[207]), along with key UK trading partners such as France, Ireland, and The Netherlands; there are several EU nations which do not adopt the mutual recognition aspect. It is, however, likely that the nations that do will continue to respect the views of ICO when approving applications; but others could possess differing requirements to be successful in a BCR application, which could lead to another lengthy application process to be certified with another authority.

[203] GDPR Articles 46(b) & Article 47
[204] GDPR Article 26(2)
[205] GDPR Article 56
[206] 'Binding corporate rules' (ICO no date): https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/
[207] J.Dipple-Johnstone, 'Changes to Binding Corporate Rules applications to the ICO' (ICO 20 November 2017): https://iconewsblog.org.uk/2017/11/20/changes-to-binding-corporate-rules-applications-to-the-ico/

It is worthwhile noticing the key omission from this mutual recognition system is Germany, the largest economy within the EU and the UK's top import, and second highest export partner[208]. This could spell difficulties should a hard Brexit occur due to the influence Germany possesses within the EU. Indeed, their hesitation to mutually recognise BCRs could lead to other nations withdrawing their commitment to allow the ICO free leave with granting BCRs which could apply within the EU, putting roughly a quarter of existing BCRs into chaos.

While it has been mentioned by the ICO that these 25% of BCRs will need to remain GDPR compliant in a post-Brexit world[209], the fact remains that the ICO is looking down the barrel of their status as an EU supervisory authority. This could result in these BCRs needing to find a new lead authority, one that could potentially be stricter in its requirements. Although the ICO has assured businesses that "no BCR authorisations will be cancelled because of Brexit"[210]; and that the aim is to continue to work with other EU supervisory authorities, regardless of how ICO finds itself in a post-Brexit world. This is due to ICO wishing to continue their position as having "leading expertise in BCR [and remaining] …continually available to the international controller and processor community"[211]. This, of course, merely shows the intention of ICO and the UK Data Protection community, and not necessarily a reality as the EU have made it clear that there will be no special dispensation given to ICO post-Brexit, hard or soft; largely due to the lack of other, non-EU nations being members such as Norway, Iceland, or Switzerland.

Overall, BCRs do carry many advantages for businesses who are based in the UK and would like to continue their operations trouble free within the EU following a hard Brexit. The issue here is the lengthy application process, strict requirements of obtaining a BCR, and the selection of a suitable lead authority to whom they can report. In addition to this, the fact that several EU Member States, including Germany, do not abide by the mutual recognition aspect could lead to further issues for businesses and more hoops to jump through.

---

[208] Office for national statistics, 2016 records: https://www.ons.gov.uk/businessindustryandtrade/internationaltrade/articles/whodoestheuktradewith/2017-02-21

[209] Dipple-Johnstone J, 'Changes to Binding Corporate Rules applications to the ICO' (ICO 20 November 2017): https://iconewsblog.org.uk/2017/11/20/changes-to-binding-corporate-rules-applications-to-the-ico/

[210] Ibid

[211] Ibid

5.3.3 Certification for businesses

One possibility available for UK businesses post-Brexit would be a relatively new concept created through the GDPR, certification. While not an entirely new concept as, "for years, certification marks and seals have served as useful signals for consumers interested in engaging with commercial entities that adhere to certain desirable principles"[212]. However, the GDPR's formal recognition of certification as a viable method is largely untested due to the age of the legislation but could prove to be a strong backup for UK businesses should other methods such as Model Clauses and BCRs be insufficient.

For the Certification method, the original basis is on making enforceable commitments in a similar vein to standard rules, but there is the potential there to utilise this guarantee for demonstrating a safeguard mechanism for data transfer purposes[213].

As with BCRs however, there are stringent requirements in order to obtain a valid certification that could, in theory, allow the free flow of personal data across the EU border. Therefore providing an approved awarding body with "all information and access to its processing activities which are necessary to conduct the certification process"[214], and then pass an assessment conducted by said body leading to a three year maximum certification which can be renewed if successful.

As with the much less stringent codes of conduct, the selected supervisory authority will be the body liable for accrediting these bodies. However, "the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012"[215] will also potentially be able to perform this task (provided that they are fully aware of extra requirements an individual State's authority may have).

---

[212] Rita Heimes, 'Top 10 operational impacts of the GDPR: Part 9 – Codes of conduct and certifications' (IAPP 24 February 2016): https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/
[213] GDPR Article 46(2)(f)
[214] Ibid
[215] GDPR Article 43(1)(b)

As mentioned, certification is a relatively new mechanism theoretically made available and could be applicable to UK businesses in a world post-hard Brexit. Indeed, such was the commotion generated around this potential interpretation that the Article 29 Working Party sought to provide draft guidelines on the accreditation of certification bodies[216] with the aim of "help[ing]...establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR"[217].

These guidelines, while not wholly binding, are likely to be followed by their respective authorities, especially following a consultation process[218]. One aspect that is likely to remain is the stressing of the point that "particular value and purpose of accreditation lies in the fact that it provides an authoritative statement of the competence of certification bodies that allows the generation of trust in the certification mechanism"[219].

It is key to point out here that the relative youth of this system may see it succumbing to the issues that mired BCRs in the early days, namely that it will "take time to establish an accreditation system, and to recruit and accredit third parties"[220]. This onus, as expected, is something for the EU to implement and not the United Kingdom in a post-hard Brexit scenario. This establishment will be a lengthy and costly process, which may be bogged down, by the bureaucratic processes found within the European Parliament and could lead to large delays to full implementation. However, if the system is used in a positive way, and parallels with the early BCR days are avoided, this mechanism could be used to alleviate many issues that could plague British businesses in a post-hard Brexit world.

[216] Article 29 Working Party, 'Draft Guidelines on the accreditation of certification bodies under regulation (EU) 2016/679' (European Commission 6 February 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877
[217] Ibid
[218] https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_en
[219] Article 29 Working Party, 'Draft Guidelines on the accreditation of certification bodies under regulation (EU) 2016/679' (European Commission 6 February 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=4987
[220] B. Treacy, GDPR series: certifications, seals and marks, P. & D.P. 2018, 18(5), 3-5

However, another drawback is that the processes for which certifications, seals, and marks can apply to need to be clarified in further detail; the EU may choose different accreditors for different sectors depending upon skill and experience. These decisions and rulings also need to consider the fact that they "need to be scalable"[221].

There is clearly the potential for this to evolve into something more than just an acknowledgement of good practices; however, as for now, this should not be wholly relied upon by UK businesses seeking to proceed uninhibited post-Brexit, but merely as a strong addition to their cause.

5.3.4 Codes of Conduct

Another mechanism, which, if used correctly, could see UK Businesses proceed with minimal hindrance following a hard Brexit, would be the use of Codes of Conduct. At its core, Codes of Conduct are simply collections of rules created by regulators but can be authorised by "associations [or] other bodies representing...controllers or processors"[222] to implement the GDPR's strict requirements. These include the concepts of fair and transparent processing, collection of personal data, and the exercising of data subject rights.

Unlike certification, the mechanism of codes of conduct are not a wholly new concept, first being brought to the fore within the Data Protection Directive as a yardstick for the "proper implementation"[223] of legislation within Member States and this has continued over into the GDPR[224], albeit with some subtle changes. One of these differences is the inclusion of conditions wherein the codes of conduct are considered to be of a particular advantage[225].

[221] Ibid
[222] GDPR Article 40(2)
[223] Directive 95/46/EC Article 27(1)
[224] GDPR Article 40
[225] Ibid (2)(a)-(k)

In regards the UK in a post-hard Brexit world, one of these sections is of some interest, namely "the transfer of personal data to third countries"[226]. This is something which could see the UK affected, when joined with another Article of the GDPR which states that in the scenario of "binding and enforceable commitments"[227] are provided by either the controller or the processor in a designated third country (which the UK would be in this scenario) that said safeguards in a code of conduct are strictly followed. This would work as an appropriate safeguard and would make transfers from the EU to the UK, and vice versa, lawful.

If applied correctly by British businesses, this mechanism can see the level of protection on a higher plane than other systems, such as model clauses, as the business choosing to rely upon this system will, according to the GDPR, be subject to monitoring[228]. This would place it on a similar level to BCRs. This monitoring should be carried out by a competent supervisory authority, likely to be the ICO based on history, but could be different if the severity of Brexit is beyond expectations.

This monitoring body will, under the guise of the GDPR, be able to "take appropriate action"[229] should a non-compliance issue be found, leading to a potential "suspension or exclusion of the...from the code"[230]. It is therefore imperative that any UK organisation wishing to utilise such a system keeps on top of their methods, systems, and can pass any stringent tests which may be imposed upon them by the authority.

Based on previous history, it is probable that if ICO is permitted to keep its status as an approved authority, the likelihood is that guidance and assistance will be provided in the first instance, and measures that are more punitive will enacted if said business fails to adhere to the guidance.

Unlike the model clause mechanism, codes of conduct would provide the added benefit of being tailor-made to the processing activity, sector of operations, or even the individual

[226] Ibid (2)(j)
[227] GDPR Article 46(2)(e)
[228] GDPR Article 41
[229] GDPR Article 41(4)
[230] Ibid

parties/branches within an organisation, allowing further flexibility. This, of course, does work as a double-edged sword; the tailoring could, in theory, allow businesses to provide a higher standard of protection, but could also leave glaring loopholes, opening themselves up to punitive measures and severely undermining the protection of data subjects.

However, for UK businesses seeking to rely on this method, there are some larger issues at play than simple poor drafting. As it stands, this mechanism is yet to be used for any transfers at all, never mind the proverbial minefield which is being created as Brexit negotiations drag on, which could lead to a great deal of uncertainty and the potential for the codes of conduct system to fall through before being fully tested.

Add to this the previously suggested notion of ICO having its status as a competent authority stripped, despite the work previously conducted and the cordial relationship it shares with the other 27 authorities. This would mean UK businesses being monitored by another EU authority, which may not have built the same relationship, or be as lenient as, ICO could be.

5.3.5 Derogations

Regardless of all the possibilities made available in a hard Brexit scenario, nothing is wholly guaranteed to work for British businesses; however, it does beg the question as to what can be expected when there is an urgent need for data to be processed.

In these scenarios, the GDPR does allow for deviation, under the rule of derogations[231], which will not come as too much of a surprise to some businesses as they are essentially the same derogations as covered under the Data Protection Directive[232].

Of course, these derogations are not protection in and of themselves, but merely act as a safety net for data transfers that are necessary despite a shortfall in protection standards either

[231] GDPR Article 49
[232] Directive 95/46/EC, Schedule 4

throughout the EU, or under any of the mechanisms. Indeed, the hesitation and reluctance to use these is best exemplified in the guidance from ICO in this manner, who believe that "derogations should be narrowly construed"[233]. This is a common term used within the British legal system, and, when used, essentially equates to using it in as few circumstances as possible and only when necessary to avoid opening the floodgates.

Fortunately, this topic is not held open to interpretation and the aspects of when a business can rely upon the mechanism of derogations are clearly laid out within the text of the GDPR itself[234], along with any other specific considerations which may be required as part of this process.

Firstly, a British business could rely upon the aspect of 'Explicit Consent'[235]. Whilst on the surface, this mechanism is rather self-explanatory, as the basis of consent as a purpose for processing is already clarified within the GDPR[236], and setting the standard at "freely given, specific, informed and unambiguous"[237] and with the ability to be withdrawn at any time. Of course, the addition here is the use of the word "explicit". While on the surface, this seems akin to adding an extra word onto an already high standard for consent and could amount to nothing, it could also make a big difference.

However, in performing their role of clarifying the GDPR, the Article 29 Working Party sought to clarify this aspect in their guidance to consent[238], stating that the "term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent"[239], further stating that this can be done via a "written statement"[240], but this

[233] 'The eighth data protection principle and international data transfers' (ICO 30 June 2017): https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf
[234] GDPR Article 49 (1)(a)-(g)
[235] GDPR Article 49(1)(a)
[236] GDPR Article 7
[237] GDPR Recital 32
[238] Article 29 Working Party, 'Guidelines on Consent under regulation 2016/679' (European Commission 28 November 2017): http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849
[239] Ibid pg 18
[240] Ibid

is “not the only way to obtain explicit consent”[241], before listing several other methods which could be used.

As expected, when undertaking such a risk with the transfer of personal data, the guidance also calls for the data subject to be adequately “informed of all the possible risks”[242] associated with said transfer to assist the subject in making their decision; in addition to the transparency requirements set out for normal transfers under the GDPR[243].

Of course, this option is available for British businesses who wish to utilise the personal data of those who are protected by the GDPR. While it is a more complex mechanism, and would require plenty of businesses to go beyond their current expectations, the potential is there to allow minimal disruption to their conduct if such a consent system is built into the bedrock of a business’ practices.

Secondly, British-based businesses could rely on the contractual aspect of the GDPR, namely the “performance of a contract”[244] or the “conclusion or performance of a contract concluded in the interest of the data subject”[245]. These two mechanisms, based purely upon the wording from the GDPR, are rather vague. These terms become vaguer when viewed through the lens of British contract law, wherein consideration is a requirement to complete a contract and merely must be something of value[246]. However, reading further into the GDPR text, the term “necessary” appears within recital 111, which places the added pressure upon the business wishing to adopt this concept.

[241] Ibid
[242] Ibid
[243] GDPR Articles 13 and 14
[244] GDPR Article 49(1)(b)
[245] GDPR Article 49(1)(c)
[246] Thomas v Thomas [1842] 2 QB 851

To go deeper into this, the Article 29 Working Party once again provide guidance on the topic[247], providing a "necessity test", like that in another paper[248]. This test required a "close and substantial connection between the data transfer and the purposes of the contract"[249]. Again, luckily, the guidance does list examples of when something is and is not necessary; listing centralising "payment and human resources management functions"[250] as not being necessary whereas "the transfer by travel agents of personal data concerning their individual clients to hotels"[251] would be necessary.

Of course, there are an innumerable number of scenarios whereby a business could opt to rely upon this method; the key is running the necessity test and hoping that the relevant supervisory authority has a similar view to the business. Otherwise, there could be a large influx of businesses falling foul of these authorities and the fines presented to them could be rather severe, especially if a business is used to conducting its operations under the guide of contract performances. This is a clear drawback to this method, as, even with the examples provided, there are too many differing cases available, and the majority of these will only be clarified through case law.

The next derogation under Article 49, "importance reasons of public interest"[252] may not be wholly applicable to British businesses but could still form a crucial safety net for some who operate within various sectors, especially financial, where the UK excels.

To be able to rely upon this derogation, a business would need to identify the public interest, and the importance of said transfer. Of course, it is important to distinguish here that just because something is interesting to the public, does not mean that its disclosure is in the public interest; it needs to be necessary much in the same way the contract performance is.

---

[247] Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (European Commission 6 February 2018): http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846
[248] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217
[249] Article 29 Working Party, 'Guidelines on Consent under regulation 2016/679' (European Commission 28 November 2017): http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849
[250] Ibid
[251] Ibid
[252] GDPR Article 49(d)

Unlike the other derogations to far, the Article 29 Working Party has yet to provide guidance on this topic, so a lot needs to be drawn from other sources, including national authorities. In this manner, the most relevant guidance for British businesses stems from ICO[253], which does apply a somewhat negative aspect for businesses hoping to potentially utilise this system. ICO mentions here that "the transfer should be in the public interest in the Member State itself rather than the third country"[254]. This would mean that, even if a British business, and indeed, the British government, deems such a transfer to be in the public interest, it is irrelevant. It is entirely down to the EU Member State to decide, which could lead to 27 differing opinions as to what equates to necessity and public interest.

Following from this is the derogation of the transfer being "necessary for the establishment, exercise or defence of legal claims"[255]. As expected, any business seeking to rely on this mechanism for a transfer should be able to demonstrate the necessity of use, and "balance the legal rights at the centre of the advice or action with the data subject's rights in relation to their personal data"[256]. While not expected for every transfer, or even for British businesses to use on a consistent basis, the fact that such a mechanism is available is invaluable for businesses who, as Article 29 Working Party use as an example[257], need to support a subsidiary based in the EU who is being sued by an employee.

There are other derogations such as "to protect the vital interests...where the data subject is physically or legally incapable of giving consent"[258]. With another being where "the transfer is made from a register…[where it] is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a

[253] 'The eighth data protection principle and international data transfers' (ICO 30 June 2017): https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf
[254] Ibid pg 26
[255] GDPR Article 49(e)
[256] Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (European Commission 6 February 2018): http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846
[257] Working Document (WP114) on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) – adopted 25 November 2005, page 15
[258] GDPR Article 49(f)

legitimate interest"[259]. However, these derogations are likely to not be used nor considered by British businesses in a hard-Brexit scenario.

One point, which is worth mentioning, which applies to all the derogations is that the need for both the controller and processor need to comply with the remainder of the GDPR. This includes the onus on controllers to identify the method of lawful processing to be conducted under Article 5, and that the data subject is rightly informed of this method of lawful processing.

As expected, with one of the more ambiguous methods of lawful processing, legitimate interests[260], the GDPR allows this somewhat in the form of a derogation[261] in the circumstance where "could not be based on a provision in Article 45 or 46"[262], including more substantial mechanisms such as BCRs and the other derogations. Of course, the use of this method is strictly controlled as it is designed as a final recourse for businesses who wish to tap into the European market. Indeed, if one is to use such a mechanism, it cannot be "repetitive, [and can only concern] a limited number of data subjects"[263] and there are no other options available. This scenario is quite literally a last resort for businesses and should not be used excessively, as it does require notifying "the [relevant] supervisory authority of the transfer"[264], and, as it stands, some authorities have outdated communication systems[265].

This is also a rather risky tactic as it could shift the balance of transfers due to the powers bestowed upon supervisory authorities who can "order the suspension of data flows to a recipient in a third country"[266] if deemed necessary. It is therefore likely that is any British business attempts to abuse this final derogation, they may find themselves completely frozen out if a supervisory authority deems the transfer repetitive or using too numerous an amount of data subjects. Neither of these standards are clarified by any authority and are open to interpretation.

[259] GDPR Article 49(g)
[260] GDPR Article 6(f)
[261] GDPR Article 49(1)
[262] Ibid
[263] Ibid
[264] Ibid
[265] For example, the Dutch authority has no email contact, so a formal letter will need to be sent
[266] GDPR Article 82

To take a strict view of this, as few as two transfers could be repetitive, and any multiple number of individuals could be too numerous. This could lead to the scenario wherein a supervisory authority can invoke such a suspension for other reasons and justify said suspension on this power.

While far from the ideal system to have in place should a hard Brexit occur, and the UK is officially declared as a third country, derogations could provide a reliving measure on a few British businesses who have intertwined ties with businesses and data subjects located on the European landmass. While not all derogations will apply to all businesses, the likelihood is that, with some clever wording and a lenient supervisory authority, derogations could help weather the storm of Brexit until a better deal is agreed between the EU and the UK for safe transfers of data. Of course, the key drawback here is that businesses need to be selective and somewhat ration their usage in order to not fall foul of the wrath of the authorities should they deem the transfers to be excessive.

5.3.6 Extraterritoriality and UK-EU Representatives

One final aspect worth breaking down is that which could befall the UK in the scenario of a hard Brexit, namely the requirement of UK businesses providing "a representative in the Union"[267] due to the extraterritorial nature of the GDPR[268].

If a hard Brexit occurs, and the UK finds itself relegated to the same situation as non-adequate nations, then the measures that are required to be taken by British businesses extend beyond simply ensuring a safe method of data transfers across the Channel.

Indeed, beyond the varying aspects of Article 45, British businesses will need to be aware of their own reach; with many large and medium-sized businesses operating to some degree within

[267] GDPR Article 27
[268] GDPR Article 3(3)

the EU, be that offering services or simply having customers who reside there, there are various rules which will need to be followed.

This requirement will apply in all scenarios, be that the softest of Brexits, EFTA membership, or the harshest of Brexits. The good news in this scenario is that the UK Data Protection Act incorporates the key aspects of the GDPR, and British businesses will have been under the supervision of the GDPR for nearly a year when such an event happens, so adaptation will have taken place. Only minor tweaks will be needed in the interim.

The only caveat, which cannot be avoided, is, as mentioned, the requirement of having a representative within the borders of the EU when such an incident happens. This can cause a large disruption to the British sector, and other third countries, who have been using the UK as their representative's location.

Of course, this requirement is not necessary for all British businesses, with the GDPR setting the scenarios when such a representative is needed[269]. As per the GDPR, a business will not be required to appoint a representative if they do not conduct "processing which is occasional, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or are a public body"[270].

Taking this in a broad concept, it is unlikely that every British business will be subject to this, but swathes of businesses will, including most of the large British financial firms, technology companies, and most of the FTSE 100. Of course, it is likely in this scenario that any company which wishes to have data flows across the Channel will need to carry out some sort of assessment to see if they fall into the categories mentioned, and then conduct the relevant changes to ensure they abide by it.

[269] GDPR Article 27(2)
[270] Ibid

This assessment is not helped by the fact that the GDPR fails to define the terms "occasional' and 'large scale', leaving them open to interpretation. This fact was acknowledged by the Article 29 Working Party, who sought to cast some like on both with two guidance papers[271], which did draw mention to these terms. However, such a term is viewed, the pressure will be on British businesses to prove their stance, and, if not choosing to have a representative, be prepared to justify it in front of as many as 27 differing Supervisory Authorities; and potentially face punitive measures from each and every one of them.

One does hope that such a measure is carefully thought out as, with the size of some British businesses, the impact financially could be astronomical should multiple authorities find them to be non-compliant with the GDPR.

[271] Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs') (European Commission 13 December 2016): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 and Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (European Commission 6 February 2018): http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846

6 CONCLUSIONS

It is clear to see that the GDPR is a highly complicated and lengthy piece of legislation, the subject of much debate and change from within the European Commission, and interpretation from outside of it. Initially passed in May 2016, whilst the UK was amidst the throws of its own heated debates one month before the referendum; it was clear from the outset that these two events would be at some sort of loggerhead.

Of course, few predicted the type of loggerhead which would form, namely the unexpected decision by the populous of the United Kingdom to vote to leave the European Union; setting in motion the chain reaction which led to this paper evaluating how British businesses who wish to continue European operations can manage.

At the time of writing, the United Kingdom has just over 7 months left on the two-year timer bestowed by Article 50 of the Treaty of Lisbon to formalise their exit from the European Union, and, as of now, the likeliest of routes is an accidental hard Brexit. However, the waters as to what can be achieved are still murky, leading to a great degree of uncertainty as to what the outcome will be. Indeed, experts are clear that "A month is a long time in politics, especially when the future of [The UK's] relationship with Europe is at stake"[272]

Due to this, one can only speculate and prepare for every possible outcome and, if negotiations thus far have revealed anything, all options are on the table due to the backtracking performed by both negotiating parties. This is regardless of if they have previously been dismissed, such as EEA membership. This is perhaps best exemplified by a recent statement from the Committee for Exiting the EU who stated that "The alternative legal processes for enabling data transfers, such as standard contractual clauses, binding corporate rules, codes of conduct, and certification mechanisms, are unsatisfactory substitutes [for adequacy]"[273]. Further mentioning that "such alternatives would represent a considerable change from the status quo, would place a

[272] B. Treacy, Expert Comment, Privacy & Data Protection Journal 2018, 18(7), 2-3
[273] Exiting the EU Committee, 7th Report – The progress of the UK's negotiations on EU withdrawal: Data, HC 1317

bureaucratic burden on individual businesses, a burden which would be prohibitive for many small businesses"[274].

One thing is for sure though; the UK is prepared for the overhaul of privacy law that was brought in formally on the 25th of May 2018, with the GDPR being applicable, and transcribed into British law through the Data Protection Act 2018. The framework for the future of British Data Protection is secured; it is the relationship with the wider European community that remains the issue.

This enacting of an enabling law is a positive sign for the British legislature, as few EU Member States had these implementing acts in place before the GDPR deadline and therefore did not default to the GDPR standards on the topics open to interpretation; others have still not been able to do so. This should be a marker of things to come with the UK when discussing their future with the EU. That they can transcribe relevant EU laws into their own laws in time, unlike some adequate states such as Canada and Switzerland, and can change their laws to better suit relationships, unlike the United States.

As with most things, the best advice is to hope for the best, but prepare for the worst; this paper sought to do that by assessing the other methods of ensuring the success of data transfers under the GDPR to allow British businesses to continue to conduct operations in the scenario that a hard Brexit is a reality.

The upside of this assessment is that, regardless of the situation relating to Brexit, there are plenty of scenarios wherein personal data will continue to flow across the English Channel unhindered; through the utilisation of one or more mechanisms prescribed by the GDPR, each with varying degrees of safety and ease for businesses. As is evidenced by the EU's plans for the GDPR, the global digital world in which we all reside is one which simply requires having a bloc such as the EU open to work with nations all over the world, especially those who reside at its doorstep.

[274] Ibid

Life on the EU's doorstep also shows promise. The UK has made it clear that they wish to have a strong relationship with the EU, regardless of how Brexit ends up, hoping to strike trade deals and other agreements beyond their departure. It is hoped that these other agreements include aspects of data protection as a minimum; and this does seem likely based on statements from an array of individuals ranging from the Information Commissioner[275], the Prime Minister[276], through to the highest echelon of power found in the United Kingdom, The Queen herself[277].

What does remain here is to what extent an agreement can be struck, and what the UK will possess. While all UK parties wish for the most advantageous deal for themselves, the 'adequacy plus' agreement, wherein the ICO has a seat on the EDPB and an adequacy ruling is provided, the stance of the EU differs greatly. The EU wishes not to be drawn into giving concessions to the UK, especially during the intense Brexit negotiations, with the chief Brexit negotiator for the EU, Michel Barnier, holding firm. There is potential for these concessions to be made after the UK's departure, but not during the negotiation process.

What is likely, however, is that the UK will apply for adequacy status as per Article 45 of the GDPR. This approach will draw on a great deal of communication and cooperation between the relevant UK power bases for data protection, both Houses of Parliament, the ICO, and whatever form a UK ambassador to the EU takes.

If all of these align, and the application uses the UK Data Protection Act as a base for the application; logic dictates that such an application will be successful. Especially when considering the current situation of Canada and Switzerland having somewhat inferior legislation, along with Japan's own recent success.

One can only draw so much out of other adequacy decrees however, as the granting of adequacy for a previous EU Member who was subject to the GDPR for 10 months is unprecedented. The

[275] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (parliament.uk meeting date 8 March 2017)
[276]Prime Minister Theresa May's speech at the 2018 Munich Security Conference, transcript: https://www.gov.uk/government/speeches/pm-speech-at-munich-security-conference-17-february-2018
[277] Statement by HRH. Queen Elizabeth II at the UK Parliament in June 2017

upside of this is that the UK can easily show their demonstration of applying the necessary standards of the GDPR on a national level, having appropriate laws in place, and having a supervisory authority who is more than capable of running the show. The potential hiccups come from other sectors, such as human rights and surveillance issues. While these have not held back the status of Canada and France, they have drawn stark criticisms of the American system and, should adequacy be granted to the UK, activists such as Schrems could immediately challenge it.

This stance is only enhanced by recent challenges along a similar vein, namely the Investigatory Powers Act, along with membership within the 'five eyes network', and the fact that previous attempts to allow data flows across the Atlantic under these tenuous circumstances could also apply to the UK, with any potential UK Privacy Shield potentially coming under fire.

Under Article 45 of the GDPR, adequacy can only be given to 'third countries', of which the UK will not be in the company of until Brexit formally happens. As such, any application to achieve this status can, and will, happen at the point when the UK leaves and not before.

This will place the UK in the precarious position of being a third country, and businesses relying upon the mechanisms until the lengthy application and review process is completed by the EU. Creating the oft-discussed cliff edge. This period can be reduced with some intelligent prior planning and drafting to ensure a smoother review process. With the EU unwilling to discuss anything to do with the relationship of the EU with the UK following Brexit until the event itself occurs, prior preparation is all which can be done.

Some have touted the possibility of the EU breaking this stance by providing the UK with 'deemed adequacy' based on their previous following of the GDPR and historical EU ties[278]. This remains purely hypothetical, with the EU not commenting on such a procedure. As such, it was not discussed in the main body of this paper, but the option is viable. According to the theory, the UK would initially be granted a temporary adequacy ruling, with planned future reviews arising from the European Commission. Whilst clearly this would be a good option for

[278] R.Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)

the UK, EU, and data flows in general, the lack of a clear comment from any influencing party puts this theory as just that, a theory, and not a viable option at the moment.

However, despite the murkiness, one thing that the UK would hope for which now stands as highly unlikely is the retention of ICO within the EDPB. While the EU freely admits the positive impact ICO have had upon the European data protection community, and their efforts on the EDPB (and previously the Article 29 Working Party)[279]; they will have no legal recourse to remain a member of this community.

This is the same outcome if the UK joins the EEA, EFTA, or seeks a relationship similar to any other existing nation with the EU. While the UK has, on numerous occasions, declared its want for the ICO to do such a thing, the fact is that the Commission is not prepared to cede this point, nor is there any rationale that would cause them to do so.

This, of course, is based largely on the fact that other nations, who have stronger and more cordial relationships with the EU, such as Norway, Iceland, and Switzerland, do not come close to having their authorities placed on the EDPB; never mind the multitude of other nations who are in possession of an adequacy ruling. The admittance of the ICO to the EDPB could open the floodgates for other applications and the already lethargic process of publishing papers and bickering within the EDPB could multiply.

The UK may have had a better chance to remain a member of the Article 29 Working Party. However, with the EDPB having substantially more power than its precursor within the EU, (with it being an official EU body[280]) and has the legal authority to act independently within the EU[281], the EU simply cannot let an outsider take a seat and potentially dictate the course taken by an EU body.

---

[279] "The Implications of the United Kingdom's withdrawal from the European Union for the Area of Freedom, Security and Justice, Committee on Civil Liberties, Justice and Home Affairs", December 2017: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/596824/IPOL_STU(2017)596824_EN.pdf

[280] GDPR Article 68(1)

[281] GDPR Article 69(1)

Leading on from this, the removal of the ICO from the EDPB does not mean an end of its EU obligations. Indeed, the EU have stressed that data protection and the associated safeguards are far too crucial to have their inclusion within EU-UK negotiations and that Brussels does see adequacy as their "preferred avenue"[282]. As other supervisory authorities within adequate nations are afforded courtesy and are expected to maintain an air of regulation over a nation's data protection policies, the ICO should behave no differently. This goes without saying, of course, as ICO, under the guidance of Ms. Denham, have seen their reputation enhanced with strong investigations into the Cambridge Analytica situation, and a detailed report into the data flow behind elections[283].

In summation, the United Kingdom has, for decades, been both the thorn in the side of the EU in terms of advancement, and a champion for furthering data protection reform across the continent, and, perhaps even globally if the incoming laws in places such as India[284], Brazil[285], and Switzerland[286] are to come to fruition.

Therefore, it is imperative that such a relationship is not tarnished and removed due to the circumstances surrounding Brexit. Such a relationship is needed to ensure the strongest possible outcome for businesses both within the British Isles and in mainland Europe. The light in these murky times is that, regardless of whether a soft or hard Brexit is the outcome in 2019, data flows can, and will, continue beyond this date one way or another; such a connection is hard to sever.

[282] 'College Meeting : European Commission endorses provisions for data flows and data protection in EU trade agreements' (European Commission 31 January 2018: http://europa.eu/rapid/press-release_MEX-18-546_en.htm

[283] Information Commissioner's Office: Democracy disrupted? Personal information and political influence 11 July 2018: https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

[284] White Paper of the Committee of Experts on a Data Protection Framework for India, November 2017

[285] Law No. 13,709, of August 14, 2018 - Provides for the protection of personal data and changes Law No. 12,965, of April 23, 2014 (the "Brazilian Internet Law")

[286] "Die Sanktionen im Entwurf zur Totalrevision des Datenschutzgesetzes Datum": 15. September 2017

7 RECOMMENDATIONS

Throughout this paper, the aim has been to remain as objectively neutral as possible and to avoid revealing any political leanings one way or another in terms of the Brexit process and the referendum that preceded the decision. The mere mention of Brexit to a British national is akin to igniting a bonfire, it is such a heated topic that many families and friendships have ended due to its discussions.

As a British national, I was afforded the opportunity to vote in the referendum and cast my vote based on what I already knew about the UK and the EU's relationship, and I stand by my vote and decision to vote to remain; it was highly disappointing that most of my compatriots did not share my assessment.

Following the research conducted for this paper and assessing all the options on the table for the United Kingdom, I hold steadfast in my view that the best possible outcome in terms of preserving the free flow of personal data across the English Channel is to reverse Brexit and keep the United Kingdom within the European Union in the same vein it has always been.

However, one must act as a realist when conducting an impartial review of the facts and an assessment of the current situation. While, in recent months and weeks, the tide is in the process of changing and the pressure is mounting on getting the British government to retract its invocation of Article 50 or hold another referendum, time is simply moving too quickly to allow such a pipe dream to become an obsession.

It is therefore my recommendation that the British government do all that it can to ensure the softest of Brexits to ensure adequacy is obtained in one form or another. Realistically, the ICO will lose their seat on the EDPB, and there will be a short period of time wherein the other mechanisms designed for third countries will need to be used for British businesses

However, anything that can be done to mitigate either the period wherein adequacy is not present, or the impact of being a third country should be pursued. This can be done either

through a great deal of prior preparation of applications, working towards the ‘deemed adequacy’ solution which was briefly touched upon earlier, or utilising the ICO to launch a campaign aimed at having more businesses compliant and aware of what will occur once the UK leaves the EU.

Time is working against these proposals, and there are a plethora of other sectors of the EU-UK relationship that also need work as negotiations are seemingly at a standstill.

What I do recommend is that a hard Brexit be avoided at all costs. It is neither beneficial for the United Kingdom nor the European Union as the impact it would have would be monumental. In a data sense, it would cause pandemonium as businesses scramble to work with the situation they find themselves in. Outside of a data sense, the economic, political, and other factors are not worth thinking about; the EU is so ingrained within the fabric of the UK that, by unravelling the thread, the entire structure could fall into disarray.

Unfortunately, unless drastic changes are made, a hard Brexit will be the outcome, one that is being led to entirely by accident and the stubbornness on both sides of the English Channel as pride takes control. However, the old adage is worthwhile to mention here; pride comes before a fall. In this case, the fall is a cliff edge.

BIBLIOGRAPHY

Legislation

UK

- Data Protection Act 2018
- HC Bill 5 2017-2019 (The Great Repeal Bill)
- Evidence to the EU Home Affairs SubCommittee, 1 February 2017: https://www.parliamentlive.tv/Event/Index/b3334d4c-93bf-4aca-9df5-666b7a72c06c
- House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Rt Hon Matt Hancock MP, Minister of State for Digital and Culture' (parliament.uk meeting date 1 February 2017)
- House of Lords, 'Brexit: the EU data protection package' (parliament.uk 18 July 2017) para 110
- House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (parliament.uk meeting date 8 March 2017)
- Investigatory Powers Act 2016
- HC Deb 15 March 2016
- Data Retention and Investigatory Powers Act 2014
- House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (parliament.uk meeting date 8 March 2017)
- House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Antony Walker, Deputy CEO, techUK; Ruth Boardman, Co-Head, International Data Protection Practice, Bird and Bird' (parliament.uk meeting date 1 February 2017)
- Information Commissioner's Office: Democracy disrupted? Personal information and political influence 11 July 2018: https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

- EU Financial Affairs Sub Committee Uncorrected oral evidence: Data sharing post Brexit, Wednesday 23 May 201810.15 am, Transcript available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-financial-affairs-subcommittee/data-sharing-post-brexit/oral/83448.html
- Exiting the EU Committee, 7th Report – The progress of the UK's negotiations on EU withdrawal: Data, HC 1317: https://publications.parliament.uk/pa/cm201719/cmselect/cmexeu/1317/131702.htm

EU and Commission papers and opinions

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
- Communication from The Commission to the European Parliament and The Council: Exchanging and Protecting Personal Data in a Globalised World
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"
- Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC
- Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, COM/2016/0594 final - 2016/0284 (COD)

- Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final (Brussels, 13.9.2017)
- Declaration of 9 May 1950: The Schuman Plan for European Integration
- House of Commons Library: Briefing Paper 7253 (13 July 2015): The 1974-75 UK Renegotiation of EEC Membership and Referendum
- Treaty on European Union, Treaty of Maastricht, 7 February 1992
- Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007
- "The Implications of the United Kingdom's withdrawal from the European Union for the Area of Freedom, Security and Justice, Committee on Civil Liberties, Justice and Home Affairs", December 2017: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/596824/IPOL_STU(2017)596824_EN.pdf
- DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
- "Data protection regulations and international data flows: Implications for trade and development", UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.
- 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland
- The Schengen acquis - Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders
- Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) (ECHR) 1950

- Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act
- Article 29 Working Party: 'Opinion 7/2014 on the protection of personal data in Quebec '(WP219, 4th June 2014)
- Statement/18/402, Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection on the state of play of the dialogue on data protection Tokyo, 31 May 2018
- 2003/821/EC: Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (Text with EEA relevance) (notified under document number C(2003) 4309)
- 2008/393/EC: Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (notified under document number C(2008) 1746)
- 2004/411/EC: Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man
- 2010/146/: Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faroese Act on processing of personal data (notified under document C(2010) 1130) (Text with EEA relevance)
- Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (European Commission 5 April 2017)
- 'College Meeting: European Commission endorses provisions for data flows and data protection in EU trade agreements' (European Commission 31 January 2018)
- EU PRESS RELEASE No 117/15
- European Commission - Press release: "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield Strasbourg, 2 February 2016"
- DRAFT MOTION FOR A RESOLUTION to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-U.S. Privacy Shield (2018/2645(RSP))

- , 'Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection' (European Commission 09 January 2018): http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245
- Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (European Commission 3 June 2003): http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf
- Article 29 Working Party, 'Draft Guidelines on the accreditation of certification bodies under regulation (EU) 2016/679' (European Commission 6 February 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877
- Article 29 Working Party, 'Guidelines on Consent under regulation 2016/679' (European Commission 28 November 2017): http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849
- Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (European Commission 6 February 2018): http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846
- Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217
- Working Document (WP114) on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) – adopted 25 November 2005, page 15
- Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs') (European Commission 13 December 2016): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 and Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (European Commission 6 February 2018): http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846
- Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000D0520

Other Bodies

- 'Agreement on the European Economic Area' (EFTA 1 August 2016): http://www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf
- EEA Joint Committee (EFTA no date) http://www.efta.int/eea/eea-institutions/eea-joint-committee
- EFTA Joint Committee meeting records: http://www.efta.int/eea/eea-institutions/eea-joint-committee/eea-joint-committee-annual-reports
- DECISION OF THE EEA JOINT COMMITTEE No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audio-visual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]
- EU Programmes with EEA EFTA Participation (EFTA no date): http://www.efta.int/eea/eu-programmes
- EC Switzerland Free Trade Agreement 22 July 1972 official journal no. L 300, 31/12/1972 p. 0189
- Federal Act on Data Protection (FADP) of 19 June 1992 (Status as of 1 January 2014)
- Ordinance to the Federal Act on Data Protection. (FADP) of 19 June 1992 (Status as of 1 January 2014) and Ordinance on Data Protection Certification (DPCO) of 28 September 2007 (Status as of 1 April 2010)
- "Die Sanktionen im Entwurf zur Totalrevision des Datenschutzgesetzes Datum": 15. September 2017
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108
- US Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (US PATRIOT Act)
- Loi du 24 juillet 2015 relative au renseignement
- Personal Information Protection and Electronic Documents Act, SC 2000, c 5
- Security of Canada Information Sharing Act S.C. 2015, c. 20, s. 2

- Standing Committee on Access to Information, Privacy and Ethics (ETHI) 42nd Parliament, 1st Session Meeting No. 52 Tuesday, March 21, 2017, 3:30 p.m. to 5:30 p.m.
- Personal Information Protection Act No.14107, 29. Mar 2016
- Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Act No. 3848 of May 12, 1986, as amended up to Act No. 13280 of March 27, 2015)
- General Data Protection Regulation' (gov.gg 16 September 2016): http://www.gov.gg/gdprnews
- United States Clarifying Lawful Overseas Use of Data Act 2018
- Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.
- White Paper of the Committee of Experts on a Data Protection Framework for India, November 2017
- U.S. Department of Commerce, Safe Harbour Privacy Principles and Related Frequently Asked Questions, July 21, 2000: https://rm.coe.int/16806af271

Cases

UK

- Thomas v Thomas [1842] 2 QB 851
- Pepper v Hart [1993] AC 593
- R. (on the application of Davis) v Secretary of State for the Home Department [2015] EWCA Civ 1185 (20 November 2015)
- Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Others [2016] UKIP Trib 15_110-CH

EU

- Google v Spain (C-131/12)
- Schrems v Data Protection Commissioner (C-362/14)
- Digital Rights Ireland v Commission (T-670/16)
- Maximilian Schrems v Facebook Ireland Limited (C-498/16)
- Data Protection Commissioner v Facebook Ireland Limited and another [2017] IEHC 545

Websites

- https://www.theguardian.com/legal-horizons/2017/dec/14/gdpr-the-new-data-protection-law-giving-watchdogs-a-mega-bite accessed 07.05.2018
- https://www.eugdpr.org accessed 07.05.2018
- https://ec.europa.eu/commission/priorities/digital-single-market_en accessed 07.05.2018
- What did the 'longest suicide note' say? BBC news magazine, 4 March 2010: http://news.bbc.co.uk/2/hi/uk_news/magazine/8550425.stm accessed 04.08.2018
- http://www.europarl.europa.eu/elections2014-results/en/country-results-uk-2014.html accessed 06.08.2018
- Electoral Commission, 2015 UK General Election Results: https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/uk-general-elections/2015-uk-general-election-results accessed 06.08.2018
- Conservative Party Manifesto 2015, pg 30: http://ucrel.lancs.ac.uk/wmatrix/ukmanifestos2015/localpdf/Conservatives.pdf accessed 06.08.2018
- Electoral Commission: https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information accessed 06.08.2018
- Interview with Theresa May by Jeremy Paxman: 29.05.2017: https://news.sky.com/video/may-on-brexit-no-deal-better-than-a-bad-deal-10897952 accessed 06.08.2018
- 'The European Free Trade Association' (EFTA no date): http://www.efta.int/about-efta/european-free-trade-association accessed 05.08.2018
- Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE), 26th May 2018: http://europa.eu/rapid/press-release_SPEECH-18-3962_en.htm accessed 05.08.2018
- HM Government, 'The United Kingdom's exit from and new partnership with the European Union' (gov.uk 2017): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_

data/file/589189/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Print.pdf accessed 08.08.2018

- http://ec.europa.eu/trade/policy/countries-and-regions/countries/switzerland/ accessed 07.05.2018
- https://www.netzwoche.ch/news/2017-02-16/was-den-obersten-datenschuetzer-der-schweiz-2017-beschaeftigt accessed 08.06.2018
- Droit de la protection des donneés: Fin de la première étape de la révision: https://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-04-13.aspx?lang=1036 accessed 08.06.2018
- House of Lords, 'Brexit: the EU data protection package' (parliament.uk 18 July 2017) https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf accessed 08.08.2018
- http://www.telegraph.co.uk/news/0/many-people-killed-terrorist-attacks-uk/ accessed 07.05.2018
- https://iapp.org/news/a/could-canada-lose-its-adequacy-standing/ accessed 28.05.2018
- 2017 report by Directorate General for Trade: http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.04.2018.pdf accessed 28.05.2018
- Statement by Canadian Prime Minister Justin Trudeau on 11.04.2018: https://www.bbc.co.uk/news/av/world-us-canada-43810913/justin-trudeau-wants-seamless-uk-trade-deal-after-brexit
- https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/ Accessed 10.05.2018
- https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_fi Accessed 10.05.2018
- 'PM speech on our future economic partnership with the European Union' (GOV.UK 2 March 2018): https://www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union accessed 04.07.2018
- https://www.nbcnews.com/tech/tech-news/chicago-tribune-los-angeles-times-block-european-users-due-gdpr-n877591 accessed 01.06.2018
- https://www.theguardian.com/business/2007/nov/04/4 accessed 07.08.2018

- http://www.europarl.europa.eu/news/en/press-room/20180611IPR05527/eu-us-privacy-shield-data-exchange-deal-us-must-comply-by-1-september-say-meps accessed 18.06.2018
- 'Binding corporate rules' (ICO no date): https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/ accessed 05.07.2018
- Dipple-Johnstone J, 'Changes to Binding Corporate Rules applications to the ICO' (ICO 20 November 2017): https://iconewsblog.org.uk/2017/11/20/changes-to-binding-corporate-rules-applications-to-the-ico/ accessed 05.07.2018
- Rita Heimes, 'Top 10 operational impacts of the GDPR: Part 9 – Codes of conduct and certifications' (IAPP 24 February 2016): https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/ accessed 07.08.2018
- https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_en accessed 09.08.2018
- 'The eighth data protection principle and international data transfers' (ICO 30 June 2017): https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf accessed 07.08.2018
- Prime Minister Theresa May's speech at the 2018 Munich Security Conference, transcript: https://www.gov.uk/government/speeches/pm-speech-at-munich-security-conference-17-february-2018 accessed 23.08.2018
- 'Global firms could pull data out of Post-Brexit UK: https://www.infosecurity-magazine.com/news/global-firms-pull-data-out-post/ accessed 23.08.2018
- https://uk.reuters.com/article/uk-britain-eu-hsbc/hsbc-shifts-european-branches-to-french-unit-control-ahead-of-brexit-idUKKBN1KT1G1 accessed 26.09.2018
- B. Katulis: "Democrats Need a Strong Alternative to Trump's 'Economic Nationalism'": https://foreignpolicy.com/2017/03/17/democrats-need-a-strong-alternative-to-trumps-economic-nationalism/ accessed: 16.10.2018

Books

- R. Jay, Guide to the General Data Protection Regulation (1st edition Sweet & Maxwell 2017)

- P. Carey, Data Protection: A Practical Guide to UK and EU Law (4th edn, OUP Oxford 2015)
- European Union Agency for Fundamental Rights & Council of Europe, Handbook on European data protection law (2014)
- C. Kuner, European Data Protection Law: Corporate Compliance and Regulation (OUP 2007)
- A. Aarnio, Reason and Authority (Ashgate 1997)
- A. Arnio, The Rational as Reasonable: A Treatise on Legal Justification (D. Reidel Publishing 1987)
- M. Van Hoecke, Law as Communication, (Hart Publishing, Oregon, 2002)

Journals and Articles

- J. Stanganelli, GDPR Territorial Scope: Location, Location, Location?, 2018
- G Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016) 6 International Data Privacy Law
- A. Salmaso, A soft Brexit: Analysis of the referendum outcomes and future possible scenarios, 2016, 10.13140/RG.2.2.27697.58723
- R. Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)
- R. Huseyin, 'News & Views – ICO gives guidance on changes to BCR applications' (2018) 18 2 (17)
- K. McCullagh; Brexit: potential trade and data implications for digital and 'f intech' industries, International Data Privacy Law, Volume 7, Issue 1, 1 February 2017, Pages 3–21
- B. Treacy, 'GDPR series: preparing for One Stop Shop' (2017) PDP 17 4 (7)
- M. Weiss & K. Archick, U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service, May 19, 2016: https://fas.org/sgp/crs/misc/R44257.pdf
- Ž. Harašić, More about teleological argumentation in law, UDK 340.132.6

- C. Kuner, D. Jerker, B. Svantesson, F. Cate, O. Lynskey & C. Millard, The global data protection implications of 'Brexit' International Data Privacy Law, Volume 6, Issue 3, 1 August 2016, Pages 167–169
- A. Murray, Data transfers between the EU and UK post Brexit?, International Data Privacy Law, Volume 7, Issue 3, 1 August 2017, Pages 149–164
- S. Bhaimia, The General Data Protection Regulation: the next generation of EU data protection, L.I.M. 2018, 18(1), 21-28
- E. Ustaran, The Future of International Data Transfers, P. & D.P. 2018, 18(6), 7-9
- K. Albrecht & K. Lust, GDPR series: international data transfers - a high level review, P. & D.P. 2017, 18(2), 14-16
- B. Treacy, GDPR series: certifications, seals and marks, Privacy & Data Protection Journal. 2018, 18(5), 3-5
- B. Treacy, Expert Comment, Privacy & Data Protection Journal 2018, 18(6), 203
- T. Katulić, From Safe Harbour to European Data Protection Reform, MIPRO 2016/ISS

GLOSSARY

2000 Decision	Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000
Article 29 Working Party	A collection of EU Member States' data protection supervisory authorities set up under the Data Protection Directive, a precursor to the EDPB
BCRs	Binding Corporate Rules
Brexit	The name adopted for the UK's exit from the EU. A portmanteau of 'Britain' and 'Exit'
CJEU	Court of Justice for the European Union

Data Protection Directive	Directive 95/46/EC on the protections of individuals with regard to the processing of personal data and the free movement of such data
DRIPA	Data Retention and Investigatory Powers Act 2014
EDPB	European Data Protection Board - The successor to the Article 29 Working Party, established under Article 68 of the GDPR
EEA	European Economic Area - A collection of the current 28 Member States of the EU and 3 of the EFTA nations (Iceland, Liechtenstein, and Norway)
EEC	European Economic Community
EFTA	European Free Trade Association
EN-ISO/IEC 17065/2012	International Organisation for Standardisation qualification: Conformity assessment - Requirements for bodies certifying products, processes and services
EU	European Union
FDPIC	The Federal Data Protection and Information Commissioner, the Swiss data protection supervisory authority
FTSE 100	A share index of the 100 companies with the highest market capitalisation on the London Stock Exchange
GDPR	General Data Protection Regulation - Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data
ICO	The Information Commissioner's Office, the UK data protection supervisory body
Irish Data Protection Authority/	The Data Protection Commission, the official Irish data protection supervisory body

Irish Authority	
MLAT	Mutual legal-assistance treaty, an agreement between nations to gather and exchange information for criminal and public law enforcement.
The Charter	The Charter of Fundamental Rights of the European Union 2012/c 326/02
The Commission	The European Commission
The Greenland Treaty	An agreement between the Member States of the European Communities, concerning Greenland's exit from the European Communities. It followed the Greenlandic referendum in 1982 in which voters supported exiting the European Community.
The Lisbon Treaty	Initially the Reform Treaty, an EU treaty signed in 2007 which reformed the European Union
The Maastricht Treaty	The Treaty on the European Union, an EU Treaty signed in 1992 which acts as one of the two treaties forming the constitutional basis of the EU
The UK	The United Kingdom of Great Britain and Northern Ireland
Third Country	A country outside of the EU
UKIP	The United Kingdom Independence Party, a political party in the UK who have the sole function of removing the UK from the EU